Chapter 6 – Data protection in the third pillar: cautious pessimism

Paul De Hert, Vagelis Papakonstantinou and Cornelia Riehle[1]

Introduction

Police and judicial databases are filled with sensitive information, as all police data on persons can be considered sensitive, whether its use violates privacy or not. Depending on the context, the mere fact that someone appears in a police database may in itself be sensitive information. Nevertheless, most citizens are unaware of the extent to which their personal data are processed by police and judicial authorities. This naivety plays into the hands of those who favour (new) security policies that infringe fundamental rights.[2]

Data protection rules with specific guarantees originally developed in the 1970s to complement traditional privacy protection. However, the essence of current data protection is most adequately reflected by Article 8 Charter of Fundamental Rights of the European Union, where data protection is introduced as a fundamental right separate from the right to privacy. According to Article 8(2) of the Charter:

> *data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

The Charter's Article 8(3) states that '[c]ompliance with these rules shall be subject to control by an independent authority'.

Although data protection rules and data protection authorities control the processing of personal data by police forces in Europe, processing of personal data by judicial authorities has traditionally received little attention. This focus of personal data protection on police data has a certain logic. On the one hand, the presence of magistrates makes data protection guarantees less needed and data protection authorities more reluctant to interfere with the work of what is a separate constitutional branch. On the other hand, it has to be noted that data used in the criminal process are already controlled by the parties involved, who can challenge their correctness. As police use of personal data cannot always be

challenged by the parties, because it does not always lead to court procedure, specific control is a necessity. The urgency of this necessity is heightened when police forces start exchanging their own data with foreign colleagues or with supranational bodies, such as Interpol or Europol. If wrong or inaccurate, data can be corrected in a closed context (eg, a national state). The situation is different in an open system where actors ignore the use of data by other actors. The EU is gradually involving itself in data protection in general and in data protection of personal police and justice data in particular, in the framework of the more intense cooperation between police and judicial actors[3] required by a closer Union. The cooperation between police and judicial authorities at EU level has indeed become the focus of legal activity and discussions within Europe, and it is foreseen as an expansion of the cross-border exchange of information, sharing data stored in national files subject to the principle of availability.

For institutional reasons, the 1995 EC directive on data protection excluded from its scope the processing of data by justice and home affairs authorities. Before (Schengen) and after this date (Eurojust, Europol) all European initiatives involving any data processing by police and judicial actors had foreseen specific data protection rules, resulting in a fragmented body of regulations. In October 2005, the European Commission finally presented a proposal for a Council framework decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters (the framework decision). Nevertheless, we would be surprised if this proposal, once voted, succeeded in guaranteeing a more harmonised set of regulations and strengthened civil liberties in Europe. Today's times are not well suited for privacy-friendly regulations, and there is actually some ground for sceptics advising not to regulate today but to wait for more balanced times.[4] This position contrasts with the position taken by the European Data Protection Supervisor (EDPS) in 2006. Recognising the negative current debate – in which data protection and privacy advocates are wrongly criticised for hindering security policies – he urges rapid adoption of a framework decision on data protection in the area of justice and home affairs (the third pillar) to accommodate and balance newly proposed security policies (such as the principle of availability (infra)) that infringe human rights and to establish a coherent framework before these new policies and the instruments that relate to them are developed.[5]

This chapter offers an overview of the beginnings of data protection and its legal and institutional development on the international level and the level of the EU, outlining initiatives for the exchange of data within police and

judicial cooperation in criminal matters, as well as the lack of a proportional development of data protection regulations in the field. The chapter concludes with a critical assessment of the proposed framework decision.

Development of national data protection

Modern data protection was first discussed in the US in the 1960s, for two major reasons,[6] one technical and the other socio-political. Firstly, the development of computers offered a new dimension to the processing and storing of data, proportional to the increasing use of computers in the public and private sectors. Secondly, the Civil Rights Movement was calling for profound changes within society, combined with an increasing fear of governmental surveillance – a 'Big Brother' – by means of this new tool.[7] The concerns for personal data, identified by US scholars, were shortly after mirrored in Europe[8], leading to legislative action. The first ever law on data protection was enacted by the German Federal State of Hesse in October 1970. It was followed by national data protection laws in Sweden (1973), Germany (1976), France (1978), Denmark (1978), Norway (1978), Austria (1978) and Luxembourg (1979). None of these initial laws could be based on any role model; they all had to be innovative in their own right. In the following years, data protection legislation was enacted by the United Kingdom (1984), Finland (1987), the Netherlands (1988), Portugal (1991), Spain (1992), Belgium (1992), Italy and Greece (1997).[9]

All these European laws regulate data protection in general, including in their scope the (electronic) processing of personal data in both the private and public sectors.[10] This comprehensive approach contrasts with the more specific strategy followed in the US and other non-European states, where data protection is regulated only for certain fields, eg, credit reporting[11] or debt collection[12]. Although this sector-specific approach might allow for the adoption of more differentiated sets of rules, it has the disadvantage of creating loopholes in the legislation. It has to be noted, nevertheless, that in recent years most European countries have complemented their general data protection laws with more sector-specific laws, for instance in the area of telecommunications, employment or video surveillance.

All European laws apply to the automatic processing of personal data, excluding, therefore, personal data manually processed and not held in a relevant filing system (for instance data kept in unstructured bundles in boxes). Although all European laws apply to the processing of data of individuals, only some of them extend the protection to the data of legal entities. The right to data protection applies to all personal data. It is not limited to data related to the private or

family life of a person, as there is general consensus on the idea that, due to modern technology, no data can, per se, be considered harmless[13]. However, EU member states have developed their data protection legislation from opposing perspectives: whereas some countries, eg, Germany and Austria, assume that the processing of data is prohibited if not explicitly permitted, others, such as France, generally permit the processing of data unless specifically prohibited.

Development of European data protection[14]

The 1981 Council of Europe Convention and its recommendations

In 1981, the first European-wide common 'model law' was introduced: the Council of Europe's Convention for the Protection of Individuals with regard to automatic processing of personal data (known as the 1981 Convention)[15], which came into force on 1 October 1985 for the members who had ratified it. The Convention was the first internationally binding instrument on data protection and formed an important point of orientation for all the subsequent national data protection laws.

Its aim is to protect the individual against abuses that may accompany the collection and processing of personal data. At the same time, it seeks to regulate the cross-border flows of personal data. According to Article 2(a) of the Convention, '"personal data" means any information relating to an identified or identifiable individual ("data subject")'. The Convention is applicable to automated personal data files and automatic processing of personal data in the public and private sectors. In addition to providing guarantees in relation to the collection and processing of personal data, it also outlaws the processing of 'sensitive' data on a person's race, politics, health, religion, sexual life, criminal record, etc, in the absence of proper legal safeguards. It enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions to the rights laid down in the Convention are only possible when overriding interests (eg, protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences) are at stake. The Convention also imposes some restrictions on transborder flows of personal data to countries where legal regulation does not provide equivalent protection.

The Council of Europe Convention creates the possibility for the member states to extend its scope to personal data files not processed (ie, collected and further used) automatically. This possibility becomes binding in the European directive, as we will see below. There is yet another striking difference between the 1980 OECD Guidelines and the 1981 Council of Europe Convention: whereas the

former does not refer to the idea of supervisory data protection committees, the latter introduces those committees as a way of permitting international data protection cooperation.[16]

The human rights approach to data protection in the 1981 Convention is undisputed. Indeed, no reference is made to economic reasons to harmonise data protection rules. Moreover, hard rules, such as the principled prohibition from processing sensitive personal data on top of the 'normal' protection of personal data, suggest a genuine concern for privacy and values, such as equality and non-discrimination.[17]

The 1981 Convention has been amended by two additional protocols. The first concerns the provision for supervisory authorities responsible for ensuring compliance with the measures in domestic law giving effect to the Convention. Furthermore, the same protocol provides that transfer of data to recipients not subject to the Convention shall only be possible if an adequate level of protection is assured.[18] The second protocol amends the Convention by allowing the European Communities to accede as such[19], because, before the amendment, only states could be parties.

The Convention is open to any country, including those which are not members of the Council of Europe,[20] and to date it has been ratified by 37 member states[21]. It still remains the only binding international legal instrument with a worldwide scope of application in this field.

In addition, the Convention and its amending protocols have continuously influenced European regulation in other contexts such as, for instance, the discussions concerning the Schengen Agreement of 14 June 1985 and its implementing Convention of 1990.[22]

Recommendation No R (87) 15 and Recommendation No (92)1

Several non-binding recommendations have been enacted by the Council of Europe to apply the general data protection principles of the 1981 Convention to specific areas of interest.[23]

Special indication for the field of police and judicial cooperation was given in the Council of Europe's Recommendation No R (87) 15 regulating the use of personal data in the police sector (Recommendation No R (87) 15)[24], which had particular significance for the later discussions on the Schengen Convention. The principles contained in the recommendation apply to the collection,

storage, use and communication of personal data for purposes subject to automatic processing. 'Personal data' covers any information relating to an identified or identifiable individual.[25] The collection of personal data for police purposes should be limited to such extent as is necessary for the prevention of a real danger or the suppression of a specific criminal offence, any exception to this provision requiring specific national legislation. The recommendation proposes several guidelines for the communication of police data to third parties (other public bodies, private parties, and foreign authorities). Like the 1981 Convention, the recommendation asks for the prohibition of the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations proscribed by law.[26]

Additionally, the recommendation asks for each member state to have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained within it.

In 1992, another important recommendation saw the light: Recommendation (92)1 on the use of DNA analysis within the framework of the criminal justice system. This recommendation applies to the collection of samples and use of DNA analysis for the purposes of the identification of a suspect or any other individual within the framework of the investigation and prosecution of criminal offences. It regulates the taking, use and storage of samples collected for DNA analysis, recourse to DNA analysis, the accreditation of laboratories and institutions and control of DNA analysis, for which member states are asked to standardise their methods. Transborder communication on the conclusions of DNA analysis should only be carried out between states complying with the provisions of the recommendation and, in particular, in accordance with the relevant international treaties on exchange of information in criminal matters and with Article 12 of the 1981 Convention. With regard to data protection, the recommendation refers to the standards laid down in the 1981 Convention and in the recommendations on data protection and, particularly, Recommendation No R (87) 15.

Recommendation No R (87) 15 remains a crucial instrument for understanding data protection in the sphere of justice and home affairs. We believe that it should be a starting point for all initiatives within the EU aiming to create more binding rules. It is, however, questionable whether this starting point can be maintained without modification, as the general tone of the recommendation is one of reactive and prudent policing, whereas today's police models are based

on more proactive concepts, such as profiling and the use of intelligence.[27] Guidelines in the recommendation limiting police data gathering to what is necessary to prevent (only) 'real' danger[28] are far too restrictive for contemporary police practices, or, to put it differently, they create a tension with some of the claims voiced by the security community.

Recommendation No R (87) 15 has already been evaluated three times (in 1994, 1998 and 2002 respectively), and evaluation will continue on a four-yearly basis.[29] The third (most recent and available at the time of this chapter) evaluation report focused mainly on the issues of distinction between judicial and police data (that have become increasingly blurred in the meantime), the use of files (distinction between permanent files and ad hoc files for particular crimes), the finality principle (further use of ad hoc files), data quality (categories of persons on whom data may be stored, length of storage and data deletion) and data transfers to third countries (which do not ensure an adequate level of protection). Nevertheless,

> *this third evaluation should not recommend any revision of Recommendation No. R (87) 15 regulating the use of personal data in the police sector, in view of the fact that it was considered that the principles laid down by this Recommendation are still relevant today and continue to provide a basis for the elaboration of regulations on this issue and serve as the point of reference for any activities in this field*.

Development of data protection in the EU

An initial lack of interest and data protection

The European Commission has dealt with questions of automatic data processing since the beginning of the 1970s as indicated, for instance, by the 1973 communication of the Commission to the Council on the Community Policy on Data Protection.[30] Data protection, however, only became an issue in 1977.[31] Meanwhile, the European Parliament had also begun to be interested in the automatic processing of data and, contrary to the Commission, it was, from the beginning, also concerned about data protection issues. In 1974, the European Parliament asked for a directive on data processing and freedom,[32] and in 1976 it requested its Committee on Legal Affairs to establish a catalogue of measures for data protection.[33] In 1979, the European Parliament adopted a resolution,[34] which asked the Commission to establish provisions for data protection. However, the Commission did not respond to this resolution, referring instead to the contemporaneous establishment of the Convention on Data Protection of the Council of Europe.

With regard to the activity of the European Community in this area, the Commission did not change its passive and inactive attitude. Although several reports and initiatives[35] underlined the necessity of a regulation of the European Communities, no concrete actions were taken apart from some diffident attempts in 1985, such as the establishment of the Legal Observatory, which did not bear any results. Up until 1989, no legally binding provisions had been established for data protection by the European Communities, which offered a rather incomplete and incoherent picture in the field. Some member states still did not have any data protection laws at all (Belgium, Spain, Italy, Greece), and the laws that had been established by the other member states varied immensely. As Convention 108 was implemented in national law, differences in detail on the national level did not disappear, but, instead, became more apparent. The substantive provisions and procedural requirements giving effect to the same basic principles could be quite different.

This phenomenon threatened the development of the internal market in the EU, especially where the delivery of public or private services depended on the processing of personal data and the use of information technology, either nationally or across borders. Member states without any regulations could provide data at a reduced rate, resulting in different market conditions. Further disadvantages arose for cross-border businesses within the European Community. Finally, the principle of the European Community as an area without borders, reinforced by the Single European Act of 28 February 1986,[36] asked for a common binding EC-wide regulation. Whereas the European Parliament did not have the power to implement it, the Commission seemed to lack the will to do so.

Schengen and Prüm

The first European-wide regulations in the field of data protection developed outside the European Community, in the framework of the Schengen process. Beginning with the 1985 Schengen Agreement,[37] and the Convention of 1990 implementing the Schengen Agreement,[38] the so-called 'Schengen Area' opened new possibilities for the processing and protection of data. The Schengen Convention represented not only the abolition of checks at internal borders, but also various new regulations for the communication of personal data. In this sense, it contained major improvements, such as rules on police exchange of data, cross-border surveillance and hot pursuit across the national borders. Furthermore, it established the Schengen Information System (SIS).

The importance of the Schengen Convention for data protection is considerable. Firstly, Schengen forced countries such as Belgium, which until then did not have a national data protection law, to adopt one. Each contracting party was supposed to adopt those national provisions necessary to achieve a level of protection at least equal to that resulting from the 1981 Convention (Article 126 Convention implementing the Schengen Agreement).

Secondly, there is an important role for data protection. General questions of data protection are answered by a reference to the Council of Europe's Convention of 1981 and to Recommendation No R (87) 15. In addition, specific questions of data protection are answered in concreto in the Convention. Most aspects of data exchange, including non-digital data exchange, have been complemented with data protection provisions.[39] Regulations on the protection of data have been made under Chapter III of the Schengen Convention, stating, in Article 117, that

> *a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in accordance with Council of Europe's Recommendation No. R (87) 15 regulating the use of personal data in the police sector shall be achieved.*

Specific rules regarding police cooperation and the exchange of personal data under the Schengen Convention were provided for in Article 129, which also refers to Recommendation No R (87) 15.

Thirdly, Schengen established the Schengen Joint Supervisory Authority (JSA) composed of representatives of national supervisory authorities and competent for monitoring the application of the Convention's provisions relating to the SIS, to deliver opinions and to harmonise its legal practice and interpretation at national level.[40] With Schengen, the idea that international data sharing had to be complemented with international cooperation regarding data protection became reality. The Schengen JSA has served as a model for the design of the other joint supervisory authorities that are currently working in the third pillar (infra).

The Schengen Convention is, however, not a data protection instrument in itself. On the contrary, it wants to facilitate data exchange between law enforcement actors and, in that respect, it has been groundbreaking. Article 39 of the

Convention contains a very strong suggestion, according to which ordinary police officers are allowed to exchange police data without the intervention of the magistrates, as had been the rule in the traditional European law of criminal cooperation. Article 39, paragraph 1 of the Schengen Convention states that

> *The Contracting Parties undertake to ensure that their police authorities shall, in compliance with national law and within the scope of their powers, assist each other for the purposes of preventing and detecting criminal offences, in so far as national law does not stipulate that the request has to be made and channelled via the judicial authorities and provided that the request or the implementation thereof does not involve the application of measures of constraint by the requested Contracting Party. Where the requested police authorities do not have the power to deal with a request, they shall forward it to the competent authorities.*

Of course, there are barriers to free exchange of police data in this provision, but they proved to be more or less formal, since most national legislation did not explicitly contain regulations on the division of labour between the police and the judiciary regarding cross-border exchanges of data.[41] In countries such as Belgium, the Schengen Convention was, therefore, seen as a sui generis legal basis for the police to exchange data,[42] although the second paragraph of the Convention bears a limitation to this practice that is convincingly clear to all actors involved and has, therefore, gained the status of ius commune in police practices:

> *Written information provided by the requested Contracting Party under paragraph 1 may not be used by the requesting Contracting Party as evidence of the offence charged other than with the consent of the competent judicial authorities of the requested Contracting Party.*

The Convention also introduced the Schengen Information System (SIS): a computer-based tool containing different categories of data on persons and objects (missing persons, wanted persons, stolen vehicle or firearms, etc) which are signalled by national central police authorities. Where a local law enforcement authority finds the objects (through a routine road check, for example), it has to take action associated with the alert (arresting the person, seizing the vehicle, etc). The SIS is, however, more than just a police tool. The alert system can also be used for border checks and other customs checks, for traditional judicial cooperation, for use by secret services and for the purposes of issuing visas, residence permits and the administration of legislation on aliens.

The Schengen alert system is based on a hit/no hit logic. A police officer searching the database will only know whether a vehicle or a person is registered, but without further inquiry he or she will not know much more, but will have to make further inquiries using other channels. Hence, the full file is not transmitted in the system. This goes some way towards protecting a data subject's privacy. However, there is a certain risk: that a hit indicates that someone is 'in' a police database and this may already be sensitive information. It is possible to think of situations in which knowledge of a hit is more risky than full knowledge of a file.[43]

The 2005 Prüm Treaty

We will return to the Schengen machinery below. Here, we wish to draw attention to the fact that whenever member states feel that cooperation and data exchange are in need of intensification, they might opt for non-EU initiatives whenever the EU is not felt to be the most appropriate forum. Schengen offers a first illustration of this. A more contemporary example is the Treaty signed between seven member states, on 27 May 2005, in Prüm[44] on enhancing cross-border cooperation, in particular to combat terrorism, cross-border crime, and illegal immigration. Like Schengen, it is a Treaty that is open to other member states.[45]

Judged by EU standards, the Treaty contains both first and third pillar ingredients. The former includes provisions regarding document advisers,[46] sky marshals,[47] and return measures.[48] The latter concerns operational police cooperation measures, such as joint patrols,[49] transferring sovereign powers to police forces of other contracting states, or assistance in the case of large-scale events.[50] Furthermore, the exchange of data concerning potential terrorist perpetrators and hooligans is regulated.[51] The most important part of the Treaty concerns the facilitation of the exchange of the following types of data: DNA profiles, fingerprints, vehicle registration (supply of any available further personal data and other information relating to the reference data will be governed by the national law, including the legal assistance rules, of the requested contracting party), non-personal and personal data.[52] For the purposes of the supply of the data, each contracting party must designate a national contact point. The Prüm Treaty introduces far-reaching measures to improve information exchange, and is open for any other member state to join. As regards the processing of personal data, each contracting party is asked to guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe's 1981 Convention and in doing so, to take account of Recommendation No R (87) 15.[53]

Although the Prüm Treaty is not uncontroversial, criticism has generally not focused on its content. Prüm is not based on a hit/no-hit system or on the principle of availability. No identifying data is transmitted. The Treaty only allows for comparison of non-identifiable data (eg, 'is DNA profile X in your database?'). Whenever identifiable data needs to be exchanged, classical channels of international cooperation in criminal law (controlled by the judiciary) have to be used.[54] The main critique presented against it is the choice of a separate instrument outside the traditional EU framework, avoiding, therefore, oversight by the European Parliament and the Court of Justice.[55] From a data protection point of view, this critique needs to be complemented with the observation that, contrary to Schengen, the Prüm Treaty does not foresee any monitoring of data exchanges by data protection authorities, nor European cooperation between them. The citizen does not find in Prüm a clear answer to the question 'how can I control the use made of my data by law enforcement authorities in other Prüm member states'? Moreover, there will not be any annual reporting on a supranational level to, for instance, the European Parliament, as is currently the case with Schengen, Eurojust and Europol.

Directive 95/46/EC (the 1995 Data Protection Directive)

In 1995, after five years of discussion, the first and major instrument for data protection was established on a European Community level by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC), which regulates the processing of personal data (defined as any information relating to an identified or identifiable natural person[56]) by laying down guidelines determining when the processing is lawful and prohibiting the processing of special categories of data (eg, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life). The directive specifies the information to be given and the rights of the data subject and establishes a series of other guidelines concerning the quality of the data, the legitimacy of the data processing, the data subject's right of access to data, the right to object to the processing of data, confidentiality and security of processing, the notification of processing to a supervisory authority and the right to a judicial remedy. Transfers of personal data from a member state to a third country are authorised only if the third country can guarantee an adequate level of protection. However, member states are also granted the right to adopt legislative measures to restrict the scope of the obligations and rights provided for in the directive, for instance for the safeguard of investigation, detection and prosecution of criminal offences. Member states are also asked to provide that one or more

public authorities (supervisory authorities) monitor the application within their territory of the provisions adopted pursuant to the directive.

However, the directive remains within the framework of the first pillar since it explicitly does not apply to the processing of data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI TEU (Article 3 (2)) – the third pillar. However, from 1995, the directive caused a wave of reform of the then existing data protection laws in the member states and, in most cases, the reforms were of a general nature, affecting data protection principles that apply to all processing, including processing done by the police and the judiciary. One could, therefore, assume, although this still needs to be demonstrated that, due to the directive, differences between legal provisions of the member states were reduced, including differences with regard to justice and home affairs.

Moreover, Under Article 29, the directive established a unique European group of data protection Commissioners (hereafter called the 'Article 29 Working Party'). The Article 29 Working Party has played an important role, not only at Community level, but also regarding third pillar issues. Indeed, although originally configured by a first pillar instrument and as a first pillar body, the Article 29 Working Party acted as the watchdog for EU data protection in general[57] – until the establishment of the European Data Protection Supervisor (EDPS) (infra) in 2004. It has established close cooperation with the EDPS, who is actually a full member of the Working Party, as well as with the JSA under the Schengen Convention.[58] It has intervened and called world attention to crucial data protection issues with third pillar relevance, such as the *PNR* case (infra) and the *Swift* case, and has advised the European Parliament on the regulation of data retetention (infra).

Article 286 TEC and Regulation (EC) No 45/2001

Although Directive 95/46/EC provided for comprehensive principles of data protection at the level of the European Community, it only applied to member states, since only member states can be addressed by a directive (Article 249 III (ex-Article 189) TEC). In consequence, the directive did not cover the processing of data by organs of the European Community. To solve this problem, the Treaty of Amsterdam introduced in 1999 into the Treaty of the European Community Article 286 (ex-Article 213b), which states that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data should apply to the institutions and bodies set up by, or on the basis of, the Treaty. In addition, Article 286 II obliged the Council

to establish an independent supervisory body responsible for monitoring the application of such Community acts by Community institutions and bodies.

One of the results of Article 286 TEC was Regulation (EC) No 45/2001 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.[59] However, like Directive 95/46/EC, the regulation does not apply to activities falling completely within the activities of the third pillar, nor do its provisions apply to bodies fully established outside the Community framework.

A second obligation resulting from Article 286 II TEC still had to be fulfilled: the establishment of an independent supervisory body responsible for monitoring the processing of personal data by the Community institutions and bodies. Regulation (EC) No 45/2001 also established the EDPS, making him responsible for monitoring the application of its provisions to all processing operations carried out by a Community institution or body. According to his mission statement,[60] the EDPS has three tasks: supervision, consultation and cooperation. With regard to the institutions of the third pillar, the EDPS has no monitoring competence, since he is not competent to monitor the processing of personal data by bodies established outside the Community framework. The task of supervision by the EDPS relates exclusively to Community institutions and bodies and it is fulfilled by carrying out prior checks, informing data subjects, hearing and investigating complaints, conducting other inquiries and taking appropriate measures where required. The competence of the EDPS does not extend to the SIS I, since the SIS operates under intergovernmental cooperation. However, the EDPS is competent for monitoring the data processing of the central part of the Schengen Information System of the second generation (SIS II), which will operate with community financing. Also, the EDPS has the specific task of supervising the Central Unit of Eurodac (Article 20 Eurodac Regulation) and, as Hijmans rightly observes, similar tasks are foreseen as regards other large-scale information systems on persons in the area of freedom, security and justice.[61] In addition, Article 46(f)(ii) Regulation (EC) No 45/2001 states that the EDPS has to cooperate with the national supervisory data protection bodies established under Title VI of the Treaty, allowing the EDPS to become an important actor in the organisation of third pillar data protection.

In his mission statement,[62] the EDPS describes his consultative task as follows:

> *Advising the Community institutions and bodies on all matters relating to the processing of personal data, including consultation on proposals for*

legislation, and monitoring new developments that have an impact on the protection of personal data.

The EDPS understands the scope of the consultative task as being much wider than his supervisory task, which only covers the processing of personal data by Community institutions or bodies. This wide interpretation was confirmed by the European Court of Justice in its orders in the so-called *PNR* case. Indeed, the Court explicitly referred to Article 41(2) Regulation 45/2001, according to which the EDPS is responsible for advising Community institutions and bodies on all matters concerning the processing of personal data. This includes, according to two orders of the Court of the First Instance, the connection between the legislation relating to data protection and that relating to the preservation of other interests. The regulation imposes on the EDPS the duty to 'cooperate' with these other players and to 'participate' in the activities of the Article 29 Working Party.

EU initiatives enhancing police and justice data exchange

The third pillar: weak and not productive?

The EU has not only established data protection regulations, mainly within the first pillar, but it has also been the forum for initiatives that are designed to make exchange and processing of personal data for law enforcement purposes easier. This development has taken place within the third pillar.

It will be recalled that criminal law has officially been an integral part of the EU constitutional order since the Treaty of Maastricht (1992). This matter was brought together under the third pillar of the EU, characterised by an intergovernmental approach (inter alia entailing a lack of judicial control by the Court of Justice, a limited role for the European Parliament, a unanimity requirement in the Council, etc).[63] The sensitive nature of criminal law resulted in a maximisation of the role of the member states (in the Council) and a minimisation of the role of the supranational institutions. Cooperation in the field of justice and home affairs is not implemented in the same way as Community policies (the common agricultural policy or regional policies, for example) are. Given the great sensitivity of matters relating to public order, the Treaty has accorded very great weight to the member states and to the bodies of the EU in which they participate directly, while the powers of the European Commission, the European Parliament and the Court of Justice have been limited for the same reason. From this viewpoint, implementation of third pillar policies is very different from the implementation of Community policies. Under the Treaty of Maastricht, the JHA lacked legal instruments, such

as 'directives' or 'regulations', which exist for Community policies, and had to use instruments specific to the third pillar, such as 'decisions' and 'framework decisions'. With the entry into force of the Treaty of Amsterdam in 1999, civil law matters, asylum and immigration became community matters, with police and judicial cooperation in criminal matters remaining within the third pillar. Notably, the Treaty of Amsterdam also made provision, in a protocol, for full integration of the Schengen acquis into the legal and institutional framework of the EU.[64]

There are traditionally two misunderstandings about the third pillar. First, the third pillar is believed to be non-productive and weak, since it lacks the powerful legal instruments of the first pillar. Nothing is less true. The legal character of first pillar 'directives' and 'regulations' and third pillar 'decisions' or 'framework decisions' is strikingly similar: both are binding upon the member states with respect to their objectives, leaving only the choice of form and method of implementation to the national authorities. Furthermore, both pillars allow for the use of binding instruments, and the only real difference between them lies in the absence in, the third pillar, of any direct effect comparable to the effect of regulations and, to a certain degree, directives.[65]

Second, another generalised misunderstanding is the idea that the third pillar is non-productive because it relies on unanimity in the Council. Even if it is true that a series of framework decisions designed to complement the mutual recognition programme that started with the European arrest warrant (EAW) framework decision of 2001 are still under debate, and although it is equally true that the Commission has no 'hard' legal instruments to sanction member states that do not implement binding third pillar instruments, the list of third pillar decisions and framework decisions already approved is impressive. For a young form of cooperation (born only in 1990) and despite the fact that it was confined until 1999 to intergovernmental cooperation, EU cooperation in criminal matters has given rise to an impressive legal and political framework. Around 200 instruments, including both legislative work and strategic documents (action plans, programmes) have been adopted. Together, they constitute the EU acquis on cooperation in criminal matters, which is the set of rules that 'candidate countries' have to implement before acceding to the EU.

From Amsterdam and Tampere to The Hague

The creation of an area of freedom, security and justice has been the most ambitious project of European integration in the past years. After only very modest steps undertaken to combat terrorism in the TREVI groups of the

1970s and 1980s,[66] and efforts made outside the Community framework, like Schengen, the speed of the development of an EU JHA policy has surprised many spectators. With the integration of the Schengen acquis into Union law by the Treaty of Amsterdam in 1999, the databases developed under its rules, the SIS and Eurodac, came under EU law. But both police cooperation and judicial cooperation benefited from the Treaty of Amsterdam mainly for another reason: it established as an objective the creation of a European area of freedom, security and justice (AFSJ). Detailing this objective into a concrete programme during its meeting in Tampere (Finland), the European Council agreed on three significant evolutions, which opened a new phase for judicial cooperation: the creation of Eurojust, the mutual recognition principle and the harmonisation of national legislations.[67]

The realisation of the 1998 Tampere Programme was later to be sped up, partly prompted by the terrorist attacks in New York and Washington, Madrid and London. Numerous initiatives for combating terrorism and serious cross-border crimes were introduced, sometimes in accelerated procedures, with the Eurojust decision and the EAW framework decision being two examples among others.[68] The Tampere Programme was replaced five years later by the 'Hague Programme' on 'freedom, security and justice', adopted at the EU Summit in Brussels on 4-5 November 2004.[69] The Hague Programme is a blueprint for EU action in the sensitive area of JHA over the next five years, and the European institutions have since begun to implement it, following an action plan.[70] Whereas the Tampere Programme was mainly a programme for legislative action, a greater emphasis on the improvement of practical law enforcement cooperation (coordinated by Europol and Eurojust) is evident in the Hague documents. As better information exchange and sharing of intelligence is urgently required, particularly in order to combat the terrorist threat to European countries, guaranteeing smooth, free data exchange in the area of the third pillar becomes one of the most important objectives.[71] To achieve this, the Hague Programme establishes that 'new technology' must be fully employed, and, therefore, since 2005, the EU has fast-tracked the rapid introduction of biometric identifiers in passports and travel documents. But the programme also introduces a principle for information exchange, the 'principle of availability', prescribing that information available to law enforcement authorities in one member state should also be made accessible to equivalent authorities from other member states, or for Europol officers. The Hague Programme states that from 1 January 2008 the 'principle of availability' will become the guiding light for access to personal data held by national law enforcement agencies in other EU member states.

As a consequence of this new emphasis on operational enhancement of police and law enforcement cooperation, several new initiatives – both inside and outside the EU framework – have been launched to improve the processing and exchange of data. With the successor of the SIS I – SIS II – and a new Visa Information System (VIS) even more data will be stored by EU institutions, and, furthermore, biometric information is now needed for residence permits and visas.

The SIS enhanced

The SIS was discussed briefly above. This database system, regulated in the Schengen Convention of 1990, has been operational since 26 March 1995. It started with only the three Benelux countries, France and Germany, but is currently used by 15 states: 13 EU member states, and, on the basis of a separate agreement, Iceland and Norway. In the near future, the SIS is to be used by at least 28 European states, as nine of the member states that joined the EU in 2004 should, depending on whether they provide sufficient technical and legal guarantees, get access to the present version of the SIS by the end of 2007 – with Cyprus being the exception to this incorporation. The UK and Ireland will also participate in part of the Schengen provisions and, even if they do not participate in the common border policy, they will thus have access to part of the SIS data. Switzerland will also accede in the future, and these four countries will join the second generation of the SIS, the SIS II.

The SIS includes more than 15 million records on objects and persons.[72] More than one million of these records concern persons who are wanted for different purposes. In accordance with the Schengen Convention, this category includes: persons wanted for arrest or extradition (Article 95); third country nationals (non-EU and non-EEA citizens) to be refused entry (Article 96); persons missing or to be placed under temporary police protection (Article 97); witnesses or other persons summoned to appear in court (Article 98); and persons (or vehicles) wanted for 'discreet surveillance' or specific checks (Article 99).

Reviewing the progress made in recent years, it is important to differentiate between the development of the SIS II (see below) and the actual amendments already made or proposed for the actual SIS. In 2001, Spain submitted a proposal for a decision (Council Decision 2005/211/JHA)[73] and a regulation (Council Regulation (EC) No 871/2004)[74] on new functionalities for the SIS. The regulation, adopted on 29 April 2004, provides for a legal basis for the information sharing by SIRENE offices,[75] introduces the possibility to add extra information stored in the SIS (eg, whether a person has escaped), and gives

visa authorities access to information on stolen identity papers.The regulation also includes the duty to make a record of every transmission of personal data, instead of every tenth transmission, which enables checking of the unlawful use of the SIS. On 24 February 2005, Council Decision 2005/211/JHA on new functions for the SIS was adopted. This decision provides for the access of Europol and Eurojust to the SIS, limited, however, to their judicial and police tasks and not including data, Article 96 (third country nationals to be refused entry), or Article 97 Schengen Convention (persons missing or to be placed under temporary police protection). Based on Article 9 of the framework decision on the European arrest warrant,[76] the issuing judicial authority may decide to launch an alert for the requested person in the SIS. Further, on 24 January 2005, the Council adopted a common position on the exchange of information on stolen and lost passports between the 'SIS countries' and Interpol.[77] By virtue of the common position, member states should, whenever they enter data on stolen passports in national databases or the SIS, immediately exchange these data with Interpol as well. Finally, in June 2005, the Council adopted a regulation to give vehicle registration authorities access to the SIS data on stolen cars.[78]

SIS II

Apart from the actual amendments with regard to the functioning of the SIS I, as described above, since 2001, member states have been preparing for the development of the 'second generation SIS' or the SIS II. The initial reason for the SIS II was the technical need to make the SIS applicable to a larger group of states, in the context of the accession of the 10 new member states to the EU on 1 May 2004. From the beginning, however, the development of the SIS II has also been used for political discussions on the new SIS requirements or functions. Between December 2001 and June 2004, political agreement was reached on the following functions: the SIS should remain a hit/no hit based information system; it should be possible to interlink alerts (allowing authorities to check whether persons/objects are registered in the SIS for different purposes); the (non-mandatory) insertion of photographs; and the (non-mandatory) insertion of fingerprints to be applicable to all alerts (Articles 95-99 Schengen Convention).[79] Regardless of the fact that on the political level the decision on the final functions of the SIS II is still awaiting adoption, technically the system is already being developed to allow for various new functions as a 'flexible tool'. Other possible new functions would include the addition of new alerts, the modification of their duration, the storage of biometric data, and the possibility to grant new authorities access to the SIS.[80]

The European Commission published three legislative proposals on the second generation SIS on 31 May 2005. In these proposals, the categories of alerts or records to be kept in the SIS remain almost unmodified. The draft regulation includes a new drafting for the registration of third country nationals into the SIS, based on a more harmonised approach for the conditions on the basis of which the registration can take place.

The discussions on the regulation by the European Parliament and the Council on the establishment, operation and use of the SIS II have been completed and the final text has already been published in the Official Journal.[81] In its preamble, the regulation states that the SIS II should permit the processing of biometric data in order to assist in the reliable identification of individuals concerned. Access to the SIS II is foreseen for authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation on third country nationals in the context of the application of the Community acquis relating to the movement of persons. Access to data entered in the SIS II and the right to search such data directly may also be exercised by national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation, as well as their coordination authorities.

With regard to data protection, the proposal refers to Directive 1995/46/EC and Regulation (EC) No 2001/45 on the processing of personal data by the Community institutions and bodies. The lawfulness of the processing of personal data by the member states will be monitored by national independent supervisory authorities, whilst the EDPS will monitor the activities of the Community institutions or bodies in relation to the processing of personal data.

Europol

Police cooperation was incorporated, through the Treaty of the European Union, into the EU's legal framework under the third pillar. The Convention, based on Article K.3 of the Treaty on European Union on the Establishment of a European Police Office (Europol Convention),[82] which formally established Europol, entered into force on 1 October 1998, following its ratification by member states, allowing Europol to start its full activities on 1 July 1999. Since then, Europol has been a central actor in third pillar developments, even if, for an outsider, it can sometimes be difficult to understand the reason why. One can

easily say that its development has taken most of the EU third pillar legislative efforts.[83]

Europol's tasks are defined to facilitate the exchange of information between the member states; to obtain, collate and analyse information and intelligence; to notify the competent authorities of the member states without delay (via the National Units) of information concerning them and of any connections identified between criminal offences; to aid investigations in the member states by forwarding all relevant information to the National Units; and to maintain a computerised system of collected information. Europol's data collection utilises mainly three systems: an automatic information system, a work files system and an index system.[84] The information system contains all available data on persons suspected or convicted of offences within Europol's mandate (Article 8(1) Europol Convention). The work files refer to data of persons as mentioned in Article 8(1) Europol Convention as well as to possible witnesses, victims, or informants of such offences (Article 10(1) Europol Convention).

With regard to data protection, each member state under its national legislation, on the one hand, and Europol when collecting, processing and utilising personal data, on the other hand, have to take the necessary measures to ensure a standard corresponding at least to that resulting from the implementation of the principles of the Council of Europe's 1981 Convention, and, in so doing, take account of Recommendation No R (87) of 17 September 1987 concerning the use of personal data in the police sector. Furthermore, each member state is obliged to designate a national supervisory body to monitor independently, in accordance with its national law, the permissibility of the input, the retrieval and any communication to Europol of personal data by the member state concerned and to examine whether the rights of the data subject are violated. Additionally, an independent joint supervisory body was set up to review the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and utilisation of the data held by Europol: the Europol Joint Supervisory Body.[85] The Joint Supervisory Body also monitors the permissibility of the transmission of data originating from Europol, and any individual has the right to request the Joint Supervisory Body to ensure that the manner in which his or her personal data have been collected, stored, processed and utilised by Europol is lawful and accurate.

The data protection provisions in the Europol Convention are exemplary, as the actual tasks of Europol are addressed with appropriate guarantees.[86] The data protection problem with Europol is another issue. First, it concerns the ever-

expanding scope of Europol,[87] a 'heavy' police tool originally limited to the most serious forms of crime and nowadays used for almost all sorts of crimes, creating a tension with the human rights principle of proportionality. Second, it is related to the Europol operations and initiatives regarding third states. Indeed, in order to widen the exchange of information, Europol has concluded over the years numerous operational agreements[88] (including the exchange of personal data) and strategic agreements[89] (not including the exchange of personal data) with several third states and organisations. The latter agreements, which are less interesting from a police point of view, are reserved for countries with a questionable human rights or data protection track record. By applying this double system, Europol appears to have been the only agency to resolve the data protection issue of international data transfers in the third pillar. However, the list of operational agreements is, without doubt, too long from a data protection perspective. Given the lack of any provisions of general application (and obviously until the framework decision[90] is published – see below), Europol has initiated exchanges with third countries that have not even made it into the list of countries providing an 'adequate' level of protection, according to the terminology and standards of the first pillar (Directive 95/46). Additionally, the actual texts that Europol concluded mostly fail to distinguish themselves when it comes to the protection of individual privacy (see, for instance, the agreement with the USA, and its inexplicably broad Articles 7 or 5).[91] While obviously such policy-making by Europol will inevitably stop in the near future (once the framework decision has been approved), for the time being it appears that Europol has appointed itself as the official EU data protection authority when it comes to international data transfers, sometimes to the detriment of individual privacy.

Eurojust

Eurojust – 'a unit (Eurojust) ... composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its legal system' – was established by the Council decision of 28 February 2002 setting up Eurojust with a view to reinforce the fight against serious crime (Eurojust Decision).[92]

The following main tasks of Eurojust were defined: to stimulate and improve the coordination of investigations and prosecutions between the competent authorities of the member states; to improve cooperation between member states, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests; and to support

the competent authorities of the member states in order to render their investigations and prosecutions more effective.

As Eurojust's activities naturally entail the exchange of personal data, the Eurojust Decision contains several provisions relating to the handling of personal data and data security. In addition, in 2005 the Council approved the Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, a text adopted unanimously by the college of Eurojust during its 21 October 2004 meeting.[93] These rules establish the main principles that apply to the processing of personal data by Eurojust, wholly or partly by automatic means: they apply to all information collected and further processed by Eurojust, that is to say, information drawn up or received by it and in its possession, concerning matters relating to the policies, activities and decisions falling within Eurojust's sphere of responsibility. However, the principles do not apply to information which has been transmitted to a national member of Eurojust exclusively in the context of his or her judicial powers. Furthermore, an independent joint supervisory body, the Eurojust Joint Supervisory Body, and an internal data protection officer were established. The Eurojust Joint Supervisory Body has a special composition compared to other joint supervisory authorities. Although its members are representatives from the different member states, they are requested to have judicial authority in their respective member state, in order to avoid the participation of members of the police administration.[94] Therefore, it is, exceptionally, not composed of representatives of the national supervisory authorities.

From a data protection perspective, Eurojust warrants two observations. The first observation concerns the issue of the legal instrument used to set it up, ie, a 'decision', a choice that shows that EU policy-makers think of 'decisions' as appropriate instruments to establish bodies with far-reaching processing capacities. Schengen and Europol had been established using 'conventions' and, since Eurojust is in many aspects the natural counterpart of Europol, one would have expected it to have an identical legal basis and, thus, be a choice for a convention. Nowadays, policy-makers favour the instrument of (framework) decisions and they have even considered amending the Europol Convention with these more flexible instruments. The second observation concerns the creation of a network of magistrates, which can be applauded. Next to traditional data protection rules, effective data protection can benefit from the classical ingredients of the law enforcement machinery, such as hierarchy and supervision by magistrates. It is unfortunate, however, that the Eurojust decision did not include an explicit power of supervision of Europol by Eurojust.[95]

Data protection issues regarding the notion of interoperability

In November 2005, the Commission presented its 'Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs' (COM (2005) 597)[96] ('the 2005 Interoperability Communication'), focusing particularly on the VIS, the SIS II and the Eurodac databases, in order to trigger an 'in-depth debate on the long-term shape and architecture of IT systems'. The purpose of this communication was

> *to highlight how, beyond their present purposes, these systems can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime.*

The 2005 Interoperability Communication is perceived more as the starting point for a large political debate than as a road map with a clearly identified aim. It contains several scenarios. One scenario is the creation of (a) European register(s) for travel documents and identity cards with biometric identifiers or for a network linking national databases of this kind, with the purpose of checking the authenticity of travel documents, ie, to check the identity of the traveller against the document in order to prevent identity fraud. Another scenario envisaged by the communication is the creation of a European Automated Fingerprints Identification System (AFIS) for criminal matters, either by establishing one large EU-wide database or by interlinking national databases.

Eurodac, the SIS II and the VIS stand central in the 2005 Interoperability Communication. The Commission notes with approval that the challenge of identifying persons in databases with millions of entries has been solved in Eurodac and in the VIS by using biometric searches, 'allowing unprecedented accuracy'.[97] The use of biometric information in the SIS II is also applauded, except for its restricted limited scope:

> *as the SIS II is being developed today, biometrics will only be used to confirm the identification of the wanted person (wanted persons meaning 'persons for whom an alert has been issued', including persons who should be refused entry) based on an alphanumerical search. When available, biometric searches would allow more accurate identification of wanted persons. However, SIS II would only store biometric information that could be legally linked to an alert in SIS II.*[98]

The communication notes that all the existing European databases, including Eurodac, are under-exploited:

> *Although the Eurodac Regulation obliges Member States to take fingerprints of all persons aged over 14 who cross their borders irregularly and cannot be turned back, the quantity of such data sent to Eurodac is a surprisingly low fraction of the total migratory flow.*[99]

Furthermore, it is observed that there is no possibility to use asylum, immigration and visa data for internal security purposes:

> *In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for all SIS II immigration and Eurodac data. This is now considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime.*[100]

The communication contains numerous 'short-term scenario' proposals to improve the use of the current databases. For instance, a more comprehensive access to the VIS and SIS II by asylum and immigration authorities is proposed to allow these 'Eurodac-authorities' to complete the assessment of asylum applications:

> *visa data can help to assess the credibility of an asylum claim and SIS II data can indicate if the asylum seeker constitutes a threat to public order or national security. A check in Eurodac, SIS II and VIS would allow asylum authorities to check the data simultaneously in the three systems*.

This recommendation is, of course, followed by the suggestion to also consider the opposite move, allowing 'authorities responsible for internal security' to access the VIS and Eurodac data:

> *As regards Eurodac, the only information available to identify a person may be the biometric information contained in Eurodac if the person suspected to have committed a crime or an act of terrorism has been registered as an asylum seeker but is not in any other database or is only registered with alphanumerical, but incorrect data (for example if that person has given a wrong identity or used forged documents). Authorities responsible for internal security could thus have access to Eurodac in well-defined cases, when there is*

> *a substantiated suspicion that the perpetrator of a serious crime has applied for asylum. This access should not be direct but through the authorities responsible for Eurodac. Access to these systems could also contribute to the identification of disaster victims and unidentified bodies.*[101]

The 2005 Interoperability Communication has been the subject of some harsh criticism.[102] The concept of interoperability it examines is not very clear, as it is naively presented as a mere technical concept and it is used, inter alia, to describe the linking of large-scale EU IT systems, such as the VIS and the SIS, as well as linking or even merging national databases (eg, DNA, AFIS). In the sensitive context of JHA, hence touching upon fundamental rights issues, and especially privacy and data protection issues, the communication suggests that the more interoperable databases are the more synergy there will be and, as a consequence, the more effective JHA policy will be. In this sense, the approach proposed by the 2005 Interoperability Communication is a perfect counter-example of the cautious approach needed in an area that touches on human rights. It reveals from the outset the Commission's deliberate choice to reduce the scope of interoperability to technical matters, and thus stresses the objective of an accurate and efficient connection of existing systems and available data. It explicitly disconnects the technical and the legal/political dimensions of interoperability, assuming that the former is neutral and the latter can come into play later or elsewhere. This way of proceeding has also been criticised by the EDPS: it leads to justifying the ends by the means.[103] Indeed, technological developments are never inevitable or neutral, which is mutatis mutandis also the case for technical interoperability. Real interoperability between different systems built for different purposes, for example between the VIS and SIS II, is questionable. The databases that the Commission deals with in its communication contain very different data and were established for different, specific purposes, allowing access to different authorities.[104] In the communication, the Commission offers poor justification as to why these databases should be used beyond their present purposes to enhance the fight against crime and illegal immigration; and there is little ground to simply assume that combining very distinct databases will help in achieving this goal. The low number of registrations in Eurodac (due to societal factors: southern EU countries do not register immigrants because of the financial implications) will not be improved by interlinking the EU databases.

The interlinking of different databases to provide data for a purpose other than that for which they have been set up ('function creep') not only contradicts the purpose-limitation principle, but it also makes the monitoring of these

processes very difficult for data protection authorities. Every move towards more interoperability requires a new analysis of its impact on data protection rights: if the purpose of a system is changed, the proportionality of measures and safeguards for the protection of fundamental rights need to be checked, too. The communication fails to address these issues.

Third pillar use of the VIS ('function creep')

Council Decision 2004/512/EC of 8 June 2004[105] establishes the VIS as a system for the exchange of visa data between member states.[106] In its 2003 guidelines,[107] the Council described the possible goals of the VIS as the improvement of the functioning of the common policy in the field of visas; internal security and the fight against terrorism; the fight against fraud; the prevention of visa shopping; an improvement of the possibilities to return illegal immigrants, and finally, the improvement of the application of the Dublin Convention.[108] On 7 January 2005, the Commission approved a regulation setting up a database of information on visa applicants,[109] extending the technical regulation of June 2004 to the VIS. On 17 October 2006, the General Secretariat of the Council issued a Presidency compromise text after the examination by the Strategic Committee on Immigration, Frontiers and Asylum/Mixed Committee (EU, Iceland/Norway/Switzerland).[110] The adoption of the VIS regulation is currently foreseen for 2007.

In the VIS, EU member states will have to store information on every visa issued; on every decision to examine an application for a visa; on each visa refused, annulled or revoked; and on each extension of a visa. This already implies the storage of information on millions of third country nationals, but the VIS will also include information on the EU and non-EU nationals inviting third country nationals. Each record is to be stored for five years. The categories of data it should contain will be: alphanumeric data on the applicant and on visas requested, issued, refused, annulled, revoked or extended; photographs; fingerprint data; links to other applications. The most recent debate on the subject concerns the age for fingerprinting children.[111]

The actual proposal of the Commission does not regulate the consequences of being registered in the VIS, and it does not explicitly prohibit visa refusals based on a record in the VIS. On 7 March 2005, the Council determined that authorities responsible for internal security should be given access to the VIS, and the Commission has since tabled a proposal granting access to both Europol and the authorities responsible for internal security, although only for clearly defined purposes.[112] Reference to this can now be found in the October 2006

text.[113] Interestingly, during the development of the system, the central unit of the VIS will be located in Strasbourg (France) and thus, hosted in the same location as the SIS II central system.[114]

In the 2005 Interoperability Communication, the inability of internal security authorities to access the VIS is considered a serious obstacle to the identification of suspected perpetrators of serious crimes. Another shortcoming of the system, according to the intelligence communities, is the fact that the VIS only deals with third country nationals:

> *The control of the identity or the legality of the entry of other categories of third-country nationals (…) e.g., holders of a long-stay visa or a residence permit (…) could also be more efficient.*

Finally, the impossibility to use the VIS to identify illegal aliens in the EU is considered 'incomplete monitoring of entry and exit of third country nationals'.[115]

As far as the VIS is concerned, the communication calls for the 'further development of existing systems and planned systems' in the following areas: (a) expanding the ability of asylum and immigration authorities to access the system; (b) extending access to authorities responsible for internal security for the purposes of preventing, detecting and investigating terrorist offences; and (c) allowing the system to be used to identify victims of (natural) disasters and unidentified bodies. The Commission also stated that 'the development of a service-oriented architecture of European IT systems would help maximise synergies', thus providing 'a way of sharing functions in a flexible and cost-efficient way without merging existing systems'. An example is given:

> *In concrete terms, one example would be to use the highly performing future AFIS part of the VIS to deliver AFIS–related services (i.e., a biometric search for other applications, such as Eurodac or, possibly, a biometric passport register). Data storage and data flows could still be strictly separated.*[116]

Third pillar initiatives to enhance data exchange and data availability

We have already discussed the EU Hague Programme, adopted on 5 November 2004, underlining its emphasis on enhanced exchange of data and on the principle of availability (meaning that if data are held then they can be shared between law enforcement agencies). The programme concerning the principle of availability will need to be fully implemented by 1 January 2008, and the

European Commission was charged with the task of preparing a proposal to achieve this objective. Of course, the principle was not completely new; it built on some existing, more concrete, ideas that were already circulating, for instance, in the European Council's declaration of 25 March 2004 on combating terrorism. The idea that data can or need to be exchanged between law enforcement authorities is as old as international criminal law and, in this sense, Article 39 1990 Schengen Convention, facilitating police exchange of data, was discussed above. With regard to the exchange of data between judicial authorities, we have observed that it was originally based on bilateral agreements, but later picked up on a supranational level through the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and other Conventions. The EU complemented this framework with the EU 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union,[117] which is particularly innovative with respect to personal data protection. Indeed, Article 23 of the 2000 Convention contains the first supranational rules establishing data protection requirements for the judiciary in their cross-border activities – even though they are very flexible and are clearly not intended to render the work of the judiciary more difficult. According to Article 23, personal data communicated under the Convention may be used by the member state to which they have been transferred (a) for the purpose of proceedings to which the Convention applies; (b) for other judicial and administrative proceedings directly related to them; (c) for preventing an immediate and serious threat to public security; (d) for any other purpose, only with the prior consent of the communicating member state, unless the member state concerned has obtained the consent of the data subject.[118]

Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol[119] was a first response to the 2004 declaration instructing the Council to take forward work on the creation of an integrated system for the exchange of information on stolen and lost passports, having recourse to the SIS and the Interpol database. It obliges the member states to ensure that the competent authorities will exchange passport data with the Interpol database on stolen travel documents, as well as enter the data in the relevant national database, and the SIS, as regards the member states participating in it. 'Passport data' means data on issued and blank passports that have been stolen, lost or misappropriated and formatted for integration into a specific information system. More concretely, 'passport data' to be exchanged with the Interpol database consist only of the passport number, country of issuance and document type. Regarding the provisions for data protection, Article 5 of the common position states that

> *The exchange of personal data in compliance with the obligation laid down in this Common Position shall take place for the purpose set out in Article 1, ensuring an adequate level of protection of personal data in the relevant Interpol Member Country and the respect for fundamental rights and liberties regarding the automatic processing of personal data. To that end, Member States shall ensure that the exchange and sharing of data takes place on the appropriate conditions and subject to the above requirements.*

We note in passing that Interpol had a bad press in the 1970s and 1980s, as certain law enforcement circles considered it ineffective and data protection circles questioned its data protection. Interpol has improved considerably in both regards and, although there is no convention regarding Interpol and data protection, sufficient detailed self-regulation is provided and an agreement with the French data protection authority has seen the light.[120] In fact, it is questionable whether more protection is achieved outside the Interpol framework.

A second initiative, also falling directly within the framework of the third pillar, was the proposal of the Kingdom of Sweden for a draft framework decision on simplifying the exchange of information and intelligence between law enforcement agencies of the EU member states, in particular as regards serious offences, including terrorist acts.[121] This so-called Swedish initiative seeks to advance cooperation by setting time limits to answer requests for information and by removing discrimination between national and intra-EU exchange of data accessible by police forces. The proposal's purpose is to establish the rules under which member states' law enforcement authorities can exchange, effectively and expeditiously, existing information and intelligence[122] for the purpose of conducting crime investigations or crime intelligence operations, in particular as regards serious offences, including terrorist acts. However, the initiative would not imply any obligation on the part of the member states to gather and store information and intelligence solely for the purpose of providing it to the competent law enforcement authorities of other member states, nor would it imply any obligation for the member states to provide information and intelligence to be used before a judicial authority as evidence, or to obtain information or intelligence by means of coercive measures. The exchange of information and intelligence is envisaged to take place via the SIRENE Bureaux, or in accordance with Articles 4(4) and 5(4) Europol Convention, or in customs matters via the central units as defined in Article 5(1) Convention on Mutual Assistance and Cooperation Between Customs Administrations, or within any other framework established at bilateral or multilateral level

among the EU member states.[123] In addition, information or intelligence not exchanged by virtue of Articles 4(4) and 5(4) Europol Convention should also be communicated to Europol, in accordance with the Europol Convention, in so far as the exchange refers to an offence or criminal activity within the Europol mandate.

On 25 January 2005, the Commission presented a white paper on exchanges of information on convictions and the effect of such convictions in the EU.[124] The paper contains a proposal to establish a computerised system for the exchange of information on convictions and disqualifications in the Union, identified by the Hague Programme as a matter of urgency. On 21 November 2005, the Council adopted the Council decision on the exchange of information extracted from criminal records,[125] which supplements and facilitates the existing mechanisms for the transmission of information on convictions based on existing conventions, pending the adoption of a computerised system of information exchange on criminal convictions between member states. On 22 December 2005, the Commission presented a proposal on the organisation and content of such exchange[126] by virtue of which national central authorities should inform the central authorities of the other member states of criminal convictions and subsequent measures in respect of nationals of those member states entered in the criminal record. Replies to requests for information from the criminal records should be sent within a certain time limit, and the personal data transferred should be used by the requesting member state only for the purpose of the criminal proceedings for which they have been requested. Regulations with regard to data protection are only specified in the preamble, where it is stated that personal data processed under the decision will be protected in accordance with the principles enacted in the Council of Europe Convention of 28 January 1981.

In pursuit of the Swedish initiative, or rather in acknowledgement of the need for third pillar data transfers cooperation, the Ministers of Justice of Germany, France, Spain, Belgium, the Czech Republic and Luxembourg and the Vice-President of the European Commission presented, on 6 June 2006, a project to connect the European criminal records. The aim of the project is to establish a secure electronic communication between national criminal records,[127] meaning, for instance, that when an information request on a French citizen issued by a German law enforcement authority is sent to the German central criminal records, the central register electronically sends the request, which has been put in a uniform format, via a European network to the French central register, where all data concerning convictions of French citizens are stored.

The information is to be sent back the same way. An automatic electronic exchange will, furthermore, be possible for information of a criminal record, on the absolute conviction of an alien, to the criminal record of his or her home country. The project, although currently supported by only a limited number of member states, is open to participation by all of them.[128]

In October 2005, the Commission made public its initiative to implement the principle of availability.[129] Availability goes beyond the exchange of information provided for by the Schengen Convention and constitutes, in this sense, a new form of cooperation previously non-existent and, hence, not part of the Schengen acquis. The proposed Council framework decision on the exchange of information under the principle of availability would apply to the processing of information prior to the commencement of a prosecution, but it would not entail any obligation to collect and store information, either with or without coercive measures, for the sole purpose of making it available to the competent authorities of other member states and Europol. 'Information' would mean existing information of the following types: DNA profiles, fingerprints, ballistics, vehicle registration information, telephone numbers and other communications data, with the exclusion of content data and traffic data unless the latter data were controlled by a designated authority, and, finally, minimum data for the identification of persons contained in civil registers. The information should be exchanged as swiftly and as easily as possible between the authorities of the member states, preferably by allowing direct online access.

As various regulations and initiatives already exist in the area, the proposed Council framework decision is supposed to provide added value, for instance, compared to the Convention of 1990 Implementing the Schengen Agreement, by introducing an obligation to reply to requests for police information exchange. With regard to the Europol Convention, improved effectiveness is expected by allowing Europol to obtain information under the principle of availability within the scope of its mandate. Furthermore, the proposal emphasises direct channels of information exchange and, following the so-called Swedish Initiative, it will introduce online access to available information and to index data for information not accessible online, after the member states' notification of information available within their jurisdictions. Finally, it needs to be noted that, although there are similarities between the proposal and the Treaty of Prüm, the proposal would be wider in scope and directly concern all member states.

Data protection problems with data exchange and data availability

Compared to setting up centralised European databases, the idea of data exchange seems to be rather innocent and selective. It is, indeed, in a selective manner, for instance, that in specific criminal cases judicial authorities should demand certain data. This is certainly true and professional secrecy can be expected to function as an adequate data protection guarantee. There are, however, serious objections to an enhanced and systematic exchange of data between member states and (even more worryingly) with third countries. First, there should be clarification of what happens to corrections, as whereas in a centralised data system they are immediately implemented, in a system of exchange one is never sure that the corrections transmitted have been, in fact, carried out. Second, in the context of exchanges between databases, there is no control of the use of data exchanged, contrary to what occurs to data in a centralised database. Sending data in this context is comparable to sending it into the void: for instance, although there can be rules stating that police data can only be used by police authorities and not immigration services officials, it is harder to control their actual use. Third, there is the problem of the retention of data: data may be outdated, but they cannot be assured. Under the Passenger Name Record (PNR) agreement, EU air companies send to US officials data that are valid only for a certain period (see below). Despite the fact that there is no update system foreseen, the agreement allows the US authorities to preserve the European passenger data for 3.5 years and, in certain specified cases, even longer.[130] One of the 34 types of information provided is 'all forms of payment information', which would include the credit card number if used for the payment of the ticket. Since it is possible to change a credit card rapidly, one can only speculate about the need to retain this data.

Just like the principle of interoperability, the principle of availability seems to undermine the data protection principle requiring data to be collected only for a specific, stated, purpose and not to be used or added to other data for any other purpose.[131] The risk is real, but we believe that the erosion of privacy and data protection principles can be avoided by building in safeguards. Moreover, it is important to see that the availability principle falls within the logic of an ever integrating Union. In 1995, Europe accepted, through Directive 95/46/EC, the idea that European firms and actors could organise themselves on a European level and transfer their data freely through a single space with a harmonised level of data protection. Today, a similar idea is elaborated with regard to the law enforcement machinery, even if it is undisputed that a policy encouraging data transfers throughout Europe makes data subjects vulnerable. Moreover, there is a clear difference between separated firms operating throughout Europe

and law enforcement actors of 25 member states not belonging to the same organisation.

Fully aware of these risks and tensions, the Commission coupled the drafting and negotiation of an 'availability framework decision' to the negotiation of a data protection framework decision (see below). Today the project to negotiate the former (and the latter) seems to have fallen off the political agenda. As the impressive series of other measures already in place or in preparation (see above) realise almost everything the law enforcement community dreams of, the added value of a general document on the principle of availability is no longer crystal clear. Recent plans to expand the Treaty of Prüm to all EU member states, discussed below, have, notably, contributed to this feeling, as they offer the possibility of exchanging DNA and other data without too many formalities. To sum up, the Hague Programme on enhanced data exchange and availability seems to have been achieved by the member states without any help from the Commission and sometimes even without the help of the EU.

The 2006 Data Retention Directive

On 15 March 2006, the Data Retention Directive was adopted by the European Parliament and the Council of the European Union.[132] The directive aims to harmonise the national provisions of the member states concerning the obligations of providers of publicly available electronic communications services and networks with respect to the retention of certain data, which are generated or processed by them, 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).[133]

The Data Retention Directive stems from a proposal introduced by the European Commission in September 2005, based on Article 95 TEU (concerning the approximation of law in the internal market). Until then, the EU legal framework in relation to data retention consisted of the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC (which translates the general principles of the Data Protection Directive into specific rules for the electronic communications sector). Articles 5, 8 and 9 of the e-Privacy Directive laid down the rules that apply to the processing by network and service providers of traffic and location data generated by using their electronic communications services. The e-Privacy Directive provided that such data must be erased or made anonymous when no longer needed for the purpose of the transmission of the communication, except for the data necessary for billing or interconnection payments, or for marketing purposes and the provision of

value-added services (subject, however, to the consent of the data subject). The legislation of most member states is in line with these principles, but several member states also adopted legislation providing for the retention of data for law enforcement purposes (ie, the prevention, investigation, detection and prosecution of criminal offences), creating differences between the member states. The differences between the various national provisions governing data retention for law enforcement purposes were considered to present an obstacle to the internal market for electronic communications, since service providers might be faced with different requirements (eg, different retention periods) in different countries. The Data Retention Directive aims precisely at harmonising these provisions to the maximum extent possible. Nevertheless, the main reason for adopting the Data Retention Directive seems to be the need for the member states' law enforcement agencies to dispose of a legal instrument that ensures the availability of data considered necessary to combat terrorism and other serious crime.

The Data Retention Directive applies to traffic and location data on both natural persons and legal entities, as well as to related data necessary to identify subscribers or users.[134] The retention period for this data is not less than six months and not more than two years from the date of the communication, meaning that operators may thus be required to retain records of all e-mails, phone calls, faxes, text messages, etc, for two years after the date of the communication. During that period, operators will need to be able to trace and identify the source, destination, location, type, date, time and duration of the communications, as well as to provide details with regard to internet, e-mail and internet telephony connections.[135] In addition, data should be retained in a way that allows for their transmission, upon request to the competent authorities, to take place 'without undue delay': not only are operators required to store huge amounts of data, but they also need to ensure that they can promptly identify and retrieve those data following a request by the competent law enforcement authorities. It is further made explicitly clear that only the competent national (law enforcement) authorities may be granted access to the retained data, and only in specific cases and in accordance with national law, each member state being responsible for defining the conditions for such access, taking into account the principles of necessity and proportionality.

With regard to the data retained, the Data Retention Directive imposes a minimum set of data security principles to be ensured by the providers of electronic communications services and networks: (a) retained data need to be of the same quality and subject to the same security and protection as data on the

network; (b) they need to be subject to appropriate technical and organisational measures against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure; (c) they need to be subject to appropriate technical and organisational measures to ensure that access to the data can only be undertaken by specially authorised personnel; and (d) they need to be destroyed at the end of the retention period, except for the data accessed and preserved.

Member states are required to designate a public authority for the monitoring of the application within their territory of the provisions adopted regarding the security of stored data, which could be, for example, the local data protection authority. Member states further need to ensure that the remedies, liabilities and sanctions provided for in the Data Protection Directive 95/46/EC are made fully applicable to the processing of data under the directive. In particular, member states should take the necessary measures to ensure that any intentional access to, or transfer of, retained data is made punishable by criminal sanctions that are effective, proportionate and dissuasive.

The directive needs to be transposed into national law by 15 September 2007, but member states may postpone application of the directive to the retention of data relating to internet access, internet telephony and e-mail, and some have already chosen this option. Before 15 September 2010, the European Commission will make an evaluation of the application of the directive and its impact on the industry and consumers and, in particular, it will need to determine whether the list of data to be retained and the periods for retention should be amended.

Problems with the 2006 Data Retention Directive

The Data Retention Directive has been the subject of extensive debate and controversy. Firstly, there has been considerable pressure exerted on the European Parliament to accept a proposal that was largely prepared in secret by the Council. The introduction of the directive followed a draft framework decision on the same issue,[136] backed only by a limited number of member states at Council level and strongly opposed by the European Parliament. The Parliament rejected the framework decision twice during the consultation procedure, until a deal with the UK Presidency of the Council and the European Commission saw the light and the same data retention obligations were introduced as first pillar legislation, ensuring in this way its full co-decision rights. The Commission, which also favoured this legal basis because it suited its preference for Community procedure, drafted a directive to be passed by an

accelerated procedure in the European Parliament and by qualified majority in the Council, using Article 95 TEC. The Parliament's approval was interpreted by some as a reversal of its own position on the question[137] and, in any case, the stronger data protection guarantees initially proposed by the European Parliament seemed to be the price to be paid for the institutional battle.

Secondly, the Data Retention Directive has also been controversial because of its significant implications for the communications industry (ISPs, telecoms operators, etc), notably because of the related privacy and cost issues.

Thirdly, there are the data protection objections. The Article 29 Working Party has called upon the member states to implement the directive with a concern for harmonisation. The Working Party is of the opinion that the directive leaves too much room for national interpretation and that, thus, the goal of harmonisation will not be achieved. Moreover, it considers that the data protection guarantees incorporated in the directive are not specific enough[138] and, although some last-minute guarantees were introduced,[139] the overall feeling remains that the directive lacks balance. The agreed minimum retention period is six months and the maximum period 24 months (Article 7), but member states may also decide on any longer term they find necessary (Article 11), which led to a Polish law allowing mandatory telephonic data retention for 15 years.[140] Most notably, the directive calls for the indiscriminate collection and retention of data on a wide range of Europeans' activities, whereas traditional police work only targets suspected persons. There has never before been a policy mandating the mass storage of information based on the possibility that it might be of interest at some point in the future.[141] Mandatory retention for the sake of law enforcement challenges the data protection principle that communications service providers should not retain their data for far longer periods than required for business purposes, and should not allow subsequent use of that data for purposes not contemplated at the time of collection.[142]

Fourthly, the current institutional problems related to the data retention issue need to be mentioned. Data retention, although serving security purposes, has been regulated, not by a framework decision (third pillar), but by a directive (first pillar). On 6 July 2006, Ireland brought an action before the European Court of Justice (Case C-301/06) claiming that the Court should annul the Data Retention Directive on the grounds that it was not adopted on an appropriate legal basis and that, therefore, the wrong instrument had been used and was not appropriate.[143] As in the *PNR* case, brought before the Court in 2005, which will be discussed in the next section, the key question in this case concerned

the applicability of Community law to the use of personal data collected by private companies for law enforcement purposes. In the *PNR* case, the Court took the view that the purpose determines the pillar. Private companies are governed by the first pillar data protection rules, but when a legal instrument forces them to process data for enforcement purposes, it has to be based on third pillar instruments which, as we have seen above, have been criticised for lacking democratic and Rechtsstaat features, such as proper parliamentary voting and proper judicial review by the European Court. Ireland (and Slovakia) expressed their intention to appeal against the Data Retention Directive in May 2006, a few months after the European Court of Justice's Advocate General's recommendation on the *PNR* case stated that the agreement was beyond the scope of Article 95, favouring with this interpretation a limited approach to the scope of Community law.[144] In October, the EDPS requested to appear before the Court of Justice in support of the defendants, as he considered that the case offered the possibility to clarify the Court judgment in the *PNR* case. According to the EDPS, a less limited interpretation of the scope of Community law would benefit the protection of data subjects.

Case-law regarding the use of data by police and judicial authorities

The growing quantity of data collected raises a number of questions that are difficult to answer solely on the basis of legal texts. Will all national authorities consent to the same standards of data collection? Can someone be refused entry into the Schengen area, just because his or her name is in the SIS files? Does data protection only exist on paper or is it enforced in practice by courts? Should we protect all data or only sensitive data? Do law enforcement authorities have a free hand when processing data because they combat crime and this is considered of the highest relevance?

Case-law regarding the SIS

One of the rare occasions where the judges have taken a strong stand on the subject matter discussed is a recent case brought before the European Court of Justice, in which the key issue was whether law enforcement authorities can refuse a person entry into the Schengen area, just because his or her name is in the SIS files.[145]

On the one hand, Directive 64/221 allows family members of third country nationals to enter the EU, and, on the other hand, the Schengen Agreement allows any member state to refuse entry into its territory to any individual on whom the system has an 'alert'. In the case at hand, two Algerians attempted

to enter Spain as family members of Spanish nationals, but Spain refused entry because of an 'alert' (placed by Germany on both persons) existing in the Schengen area. The situation illustrated the contradiction between the directive and the Schengen Agreement because, according to the first, the two Algerians should have been permitted to enter Spain, but, according to the second, Spain had the right to refuse entry into the Schengen area. The Commission filed against Spain, whose authorities claimed the rejection of entry was lawful because the measure was by virtue of the Schengen Agreement. The Court examined first the relationship between Community law and the Convention implementing the Schengen Agreement (CISA) and found that

> *the compliance of an administrative practice with the provisions of the CISA may justify the conduct of the competent national authorities only in so far as the application of the relevant provisions is compatible with the Community rules governing freedom of movement for persons.*[146]

Ultimately, the Court weighed the Schengen Agreement and the Data Protection Directive, and found in favour of the directive: the provisions of the Schengen Agreement allowing for automatic rejection were contrary to Community law and could not be applied; member states should examine the merits of each case separately (whereby the freedom of movement takes precedence) before reaching a decision.

The Court's reasoning closely resembles the right not to be judged solely on the basis of automated decisions referred to in Article 15(1) 1995 Data Protection Directive. Indeed, the Court finds that 'automatic' rejections do not seem to comply with the freedom of movement within the EU:

> *It follows that, under the mechanism provided for by the CISA, a person falling within the scope of Directive 64/221, such as a national of a third country who is the spouse of a Member State national, risks being deprived of the protection provided for by that directive where an alert has been issued for the purposes of refusing him entry.*[147]

[...] 'In such circumstances', states the judgment,

> *the Spanish authorities were not justified in refusing entry to the persons concerned without having first verified whether their presence constituted a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.*[148]

The judgment contains a serious limitation on proactive profiling techniques, which allow for persons to be blacklisted on the basis of certain characteristics identified by profiling software. Moreover, the judgment can also be interpreted as a warning: when a member state uses data transferred by another it is never 'covered' by the fact of not being responsible for entering the data. If, for instance, its authorities refuse someone entry into the territory, they must previously have carried out a concrete assessment of the danger to public order posed by the person.[149]

The PNR case

A highly significant case is the one known as the *PNR* case. Since January 2003, European airlines flying into the United States have been obliged to provide the US customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' (hereinafter 'PNR data'). Based on US laws adopted following the terrorist attacks of 9/11, airline companies are obliged to submit the data before or immediately after the airplane takes off and, if they fail to do so, they can be fined a maximum of $5,000 for each passenger whose data have not been appropriately transmitted. The PNR data comprise 34 fields of data, including not only name and address, but also contact details, such as telephone numbers, e-mail addresses, information on bank numbers and credits cards, and also on the meals ordered for the flight. The US demand for data held by European firms for billing purposes without the consent of the passengers to the transfer or a proper legal basis clearly violates European data protection regulations. The European Commission tried to solve the problem by negotiating with the US officials a series of requirements and subsequently adopting a decision on adequacy based on Article 25 EC Directive on Data Protection,[150] whose adoption meant that the Commission was convinced that the US would ensure an adequate level of data protection for the transfers. This decision enabled the Council to adopt the agreement of 17 May 2004 between the European Community and the United States of America[151] to officially allow the transfers.

When negotiating these instruments, the Commission assumed that it was competent to do so on the basis of the provisions in Community law regarding transportation and data protection. However, on 30 May 2006, the European Court of Justice annulled Council Decision 2004/496/EC and Commission Decision 2004/535/EC[152], arguing that they could not have their legal basis in EU transport policy (a first pillar provision). A careful reading of the preamble to the EU-US agreement led the Court to find that its purpose was: to enhance security, to fight against terrorism, to prevent and combat terrorism, related

crimes and other serious crimes, including organised crime; and to prevent flight from warrants or custody for those crimes. Thus, the Court held that the data transfers concerned fell within a framework established by the public authorities related to public security.[153] The Court judgment has been seen as a failure for the European Parliament, as it had launched the procedures but mainly on a different ground, namely, that Council Decision 2004/496/EC and Commission Decision 2004/535/EC accepted a disproportionate transfer of data to the United States without proper data protection guarantees. This issue was simply not addressed by the Court, which concentrated instead on the institutional arguments raised by the European Parliament. Even from this point of view, however, it is doubtful whether the result was really what the European Parliament was aiming for, as the judgment resulted in any new agreement having to be negotiated in the context of the third pillar, where the Parliament has less of a voice than in the first pillar and is, thus, excluded. Moreover, in the third pillar, the European Court of Justice exerts a high level of control, as its jurisdiction over those matters depends on whether each member state has made a declaration permitting its national courts (and not necessarily courts at the same level) to refer questions to the European Court of Justice on third pillar issues. Finally, the rejection of the 1995 Data Protection Directive as a proper legal basis has to be noted. The European Court of Justice concluded, on the one hand, that the collection of PNR data by airlines falls within the scope of Community law, but, on the other hand, it seemed to accept that if the same data are to be transferred for public security reasons they no longer need the protection of the 1995 Data Protection Directive.[154] In his initial reaction to the *PNR* judgment, the EDPS rightly declared that this reasoning creates a loophole in the protection for citizens. The judgment seemingly implies that the transmission of information to third countries or organisations from the future VIS or SIS II would escape the applicable rules of the 1995 Data Protection Directive, as long as the transmission is intended for police or public security use.

As seen above, a similar argument to the one used by the Court in the *PNR* judgment has been raised with regard to the legal basis for the directive on data retention in Ireland's and Slovakia's appeal against it before the European Court of Justice. The EDPS request to appear before the Court in support of the defendants is not only an expression of his interest in an eventual clarification of the applicability of Community law to the use of personal data collected by private companies for law enforcement purposes, but also an opportunity to oppose the argument that a first pillar proposal should not include rules on access by police and judicial authorities. The case is still pending.

Towards a framework decision on the protection of personal data

Rationale

Currently, the basic text governing data protection by law enforcement is not part of the EU law but derived from the Council of Europe, since Directive 95/46/EC does not apply to matters of justice and home affairs. We have already seen, above, that the 1981 Council of Europe Convention on data protection has indeed become the standard in the field of justice and home affairs, as the legal instruments on Schengen, Europol, Customs Information System and Eurojust all refer to it and require member states to take measures to achieve its level of protection. Today, nevertheless, there is a call for the EU to take legal action and to elaborate a new standard text on data protection in the third pillar, replacing or complementing the specific provisions governing initiatives, such as Schengen, Europol and Eurojust. Several factors account for this. Firstly, the Council of Europe's Convention regulates processing done by law enforcement authorities without taking into account the specific characteristics of the contemporary exchanges of data by police and judicial authorities and, in addition, case-law regarding privacy and data protection is slow and reticent. We subscribe to this argument, because, as already underlined, neither the 1981 Council Convention, nor its 1978 Recommendation No R (87) 15, address the consequences for data protection of new police practices, such as intelligence-led policing, so it is easy to understand that Europe is in need of a data protection framework addressing the issues raised by those practices.[155] Secondly, international data exchanges are increasing, due to further integration and facilitated by legal instruments, such as the 2006 framework decision on the exchange of information, as well as policy options, such as the availability principle and interoperability. At the same time, methods of data gathering and data exchange are also multiplying, again facilitated by EU initiatives, such as the Data Retention Directive. Thirdly, there is the will to overcome the current legal difficulty to determine whether certain processing and transfer operations in the area of justice and home affairs, especially those carried out by private actors, fall under the rules of the first or the third pillar. In the *PNR* case, the Commission argued that the regulation of the transfer of passenger data by private airlines would fall under the rules applicable to the harmonisation of the internal market (Article 95 TEC), but the Court of Justice found that the data transfer was motivated by concerns for public safety and, therefore, fell under the scope of the third pillar.[156] Fourthly, another argument is that adequate data protection supervision requires more integration of the existing supervisory bodies for Europol, Eurojust and the SIS. To varying extents their controls are based on the 1981 Convention and Recommendation No R (87) 15, but each

organ follows its own specific data protection rules incorporated into the legal instruments under which they are established.

For busy policy-makers, the third argument is probably the most convincing, since it deprives the EU of having a voice in issues with a clear European dimension. It is, nevertheless, questionable whether legislative action is generally felt to be a priority, particularly as earlier attempts to draft a framework decision were unsuccessful.[157] Some actors consider that the existing framework seems to function relatively well, and those who feel that data processing by police and justice authorities does not need too much effective control could actually see the lack of updated rules on data processing as a gift from heaven.

In fact, the real rationale behind the current initiative to draft a framework decision on the protection of personal data processed within the framework of police and judicial cooperation seems to be political pressure: the Council's promise to the European Parliament to adopt such a decision at the time of the voting on the 2006 Data Retention Directive. Additionally, its need was felt by the Commission and the Council when introducing the proposal of October 2005 for a Council framework decision on the exchange of information under the principle of availability (discussed above), a document with far-reaching data protection implications.[158] Motivated expressly by the bombings in London in 2005[159] and within a short (six-month) notice by the Council, in October 2005, the European Commission presented its proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[160]

The drafting process of the framework decision

After the submission of the proposal by the Commission in October 2005, the EDPS issued an opinion (in December 2005), and the European Parliament agreed on the 60 amendments in its report in May 2006 and adopted it in September 2006.[161] However, between November 2005 and November 2006, the Council's Multidisciplinary Group on Organised Crime (MDG) produced 29 reports substantially changing the Commission's proposal without reaching agreement on the text. A new draft was made available in November 2006.[162]

The work of the Commission and the interventions of the MDG met with little enthusiasm. The EDPS and the European Parliament, both of which felt that their views had been ignored,[163] focused part of their critique on their lack of voice during the drafting procedure: by the time the framework decision was drafted, data protection changed Directorates within the EU bureaucracy – from

DG Internal Market it moved to DG Justice and Home Affairs. This change appears to have gravely affected the 'quality' of the Commission's proposals and performance during the subsequent negotiations, which were, quite surprisingly, led by the Council's MDG, a group comprised of police officers and Ministry of Justice officials, which showed very little interest in data protection[164] and which consequently refused all involvement of data protection experts (either the Working Party or the EDPS) in the process of redrafting. Lack of consensus within the group explained why, in January 2007, the German Presidency, admitting that the Council was in a mess, asked the European Commission to go back to the drawing board and prepare a 'revised' proposal.[165] At the meeting of the Article 36 Committee on 25 and 26 January 2007, the Presidency set out a series of basic points[166] for revising the proposal, with the aim of removing outstanding reservations and making a real improvement in third pillar data protection. In March 2007, the Presidency issued its revised draft.[167] The draft was submitted to the Article 36 Committee at its meeting on 22 and 23 March 2007.

In the following section, we will discuss the content of the first versions of the draft framework decision, highlighting the main discussion points that explain why a consensus has still not been reached.

The October 2005 proposal for a Council framework decision

The original 2005 proposal was drafted by the Commission along the lines of Directive 95/46. Taking into account that a solid instrument in the field of data protection already existed, that principles and national legislations were already in place and that the architecture of control was already established (supervising authorities, both at a national and at a European level), it would have appeared inconsistent if the proposed framework decision had not at least followed the pattern of the directive.[168] Consequently, both the structure of the proposed framework decision and its approach to its subject matter has been influenced by the directive: scope and definitions in Chapter I, the general data protection principles in Chapter II, individual rights in Chapters IV, V and VI, establishment of a Supervisory Authority (to be assisted by a Register) and a Working Party in Chapter VII – only Chapter III, defining the special types of processing and data transfers (principle of availability) is entirely unprecedented.

The stated goal of the 2005 draft is twofold: to safeguard the interests of the data subjects in the area of justice and home affairs and to create a legal environment to foster trust and, hence, more cooperation without undue obstacles between the law enforcement authorities. The draft bears the following characteristics: (a)

it follows not only the pattern but also the contents of the directive, including such issues as the finality principle, the rights of data subjects, the control of personal data exports to third countries, etc; (b) the Commission seems to place emphasis on the protection of human rights; (c) the legal basis of the proposed framework decision is obscure; it also remains to be seen whether the domestic processing of member states may be governed by it; (d) the draft attempts to strike an admittedly difficult to find balance between the instruments already in effect (Schengen, Europol, Eurojust, Customs Information System);[169] (e) it also attempts to strike an equally difficult balance between its subject matter (criminal matters) and the matters that should be excluded altogether from application of its provisions (ie, state security).

Several major problems had to be dealt with in the process of drafting the framework decision. Firstly, an important difficulty was to determine the exact difference between police authorities and judicial authorities. Data protection up until now has focused mainly on controlling police processing, the judiciary being considered 'less dangerous' and less in need of control since its tasks are more limited, viz, bringing suspects before the judge, where the procedural rules of due process determine the proceedings. However, police forces have a broader task, ranging from criminal investigation, to crowd control, to political policing, a series of functions often exercised without transparency, making control and data protection more vital. Moreover, police data are sometimes based on uncertain facts or on assumptions and hearsay ('soft data'), whereas judicial information mainly concerns established facts ('hard data'). Finally, on an organisational level the traditional separation of powers and the independence of the judiciary make the control of its members by data protection authorities more than delicate.

Secondly, another problem is the differences between the police and judicial systems around Europe: several member states have specialised criminal investigation police bodies, while others do not; in some member states only the police can enforce penalties, while in most it is done by the prosecutor. The lack of harmonisation of the criminal process at European level is general, beginning with the identification and investigation of a crime until its discussion in court.

Thirdly, political and national considerations also represent a major difficulty. The 'terrorism' climate is certainly one of those considerations, pushing for as much 'availability' of data as possible, even if with the typical minimum requirements. It should be recalled that the proposed framework decision was

drafted by the Commission (Justice Directorate) but was subsequently due to go through the Council and its Committees on Crime, where the emphasis is not placed upon individual rights, but rather on police priorities. If the principle of availability can be expected to be most welcome in these circles, the data protection that comes with it is not. Finally, practically all member states have set up their own 'politics' within the crime prosecution sector, by entering into bilateral agreements for the exchange of information (police cooperation) with countries of the third world that would be unable to fulfil any requirements for 'adequacy' data protection examination. Nevertheless, for many member states the established cooperation may seem too valuable to be abandoned.

The debate regarding the scope of the framework decision

The work of the Commission was not favourably received by the member states' representatives in the Council's MDG. A first debate was triggered around the scope of the proposal, particularly concerning the question of whether the initiative applied to all processing of data by law enforcement authorities or only to processing of data with the purpose of being exchanged within the EU. The proposed draft applied to internal or domestic processing of data, as well as cross-border exchange of data, which seems convenient both from a practical and a theoretical perspective: it seems evident that the framework decision should apply to all processing within the member states, as data protection principles cannot apply at a cross-border level if they are not applied domestically beforehand. However, several member states seemed to have objected to this uniform application, suggesting that the provisions should only be implemented for international data transfers.[170] If this were the case, the police and the justice systems of each member state would maintain two databases: one for internal use (where obviously processing goes on uncontrolled or, in any event, according to national law), and one for international data transfers (where the framework decision would apply). On a practical level, this cannot work: how can the police know in advance (while setting up its databases) which data will be requested in the future by another member state? To separate data into two 'sets' is obviously not only impractical but also costly, as it requires double databases and technical infrastructure. On a more theoretical level, the question that can be raised is: what kind of processing do the member states not willing to comply with basic data protection principles execute? Also from a theoretical perspective, it needs to be highlighted that framework decisions are meant to harmonise, not to assist international exchanges between member states: the creation of double databases with one half being uncontrollably processed in each member state offers little to the purpose of harmonisation. Finally, it should be noted that, regarding questions of legal basis, the Council

Legal Service delivered an opinion whereby it confirmed that the framework decision might also apply to domestic police processing.[171]

The debate between security and privacy and its consequence for the data protection principles in the framework decision

With a new Directorate in charge of data protection and with a series of new guiding data processing principles (interoperability, availability) politically established, it is not surprising that the Commission's work was not wholeheartedly loyal to the classical data protection principles it had, until recently, backed The finality principle was brutally attacked (by the notion of 'further processing'), the principle of availability was evidently present, and police data seemed to be allowed to flow not only between different police authorities, but also other state agencies, and, indeed, even private parties(!). However, a comparative analysis of the original Commission proposal and the status of the framework decision as of November 2006 demonstrates that the MDG was able to significantly reduce the protection of individuals to the benefit of law enforcement interests. The November 2006 draft framework decision resembles only formally the initial proposal of the Commission, as each and every fundamental data protection principle has been tied to exceptions that often make it unenforceable. The finality principle has been mostly put to the test: rather than setting up databases for single purposes only, 'further processing of data' is considered lawful in a multitude of cases, among which are listed such broad categories as processing for 'the protection of rights and freedoms of a person', or when 'necessary for lawful purposes of public interest',[172] reducing to a very few cases those when police forces may not use its records (and records of other state authorities) for whichever purposes they wish.[173]

The 'accuracy' principle has also come under attack: according to the November 2006 draft framework decision, inaccurate police records (and, obviously, their use by police authorities to the detriment of individuals) shall be permitted if the police take

> *every reasonable step […] to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, for which they are further processed are erased or rectified.*[174]

Regarding international data transfers under the principle of availability,

> *Member States shall provide that appropriate measures are taken to ensure that, in cases where the controller rectifies, blocks or erases personal data*

> *following a request, a list of the suppliers and addressees of these data is produced, unless this proves impossible or involves a disproportionate effort.*[175]

In addition, all police mistakes are liability-free, because 'the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage',[176] negligence is, obviously, included.

Of course, these exceptions also have a severe impact on more secondary data protection principles. In this sense, the November 2006 draft framework decision practically abolishes the time restriction imposed by the 1995 Directive on all personal data that have fulfilled their purpose. It states that, when it comes to police data,

> *Member States shall provide that automated personal data shall be stored only as long as it is necessary for the purpose for which it was collected or further processed,*[177]

the emphasis obviously being placed here upon the expression 'further processed'.

Contrary to what could be expected in times of international terrorism and religious fundamentalism, the November 2006 draft framework decision cares very little for the police basing its processing on the religion, the origin, the political beliefs or the sexual preferences of individuals – what is known as 'sensitive data' requiring special protection. Indeed, rather than the original wording of the Commission,[178] which was formulated negatively and strictly along the lines of the directive, the MDG opted for the following:

> *In addition to the conditions laid down in Article 5, Member States shall permit 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 only when this is strictly necessary. Member States shall provide for suitable additional safeguards.*[179]

This broad wording obviously constitutes a reduction in the level of data protection for individuals in the sector where it is most needed. Indeed, it is not especially first pillar processing (by marketing companies, banks, etc) that hurts

individuals when based on sensitive data, but rather state processing (police enforcement and consequent actions).

The situation of individual rights very much resembles the data protection principles erosion in the text (see above): even though the Commission included them in its original proposal as per the acquis of the directive, the MDG seems to have undertaken positive measures to undermine them. A comparative analysis of Article 19 on the right to information, as set out in the Commission's original proposal and in the draft of the MDG of September 2006, easily proves that individuals ultimately have very restricted options when exercising their rights. The same is, unfortunately, the case with the right of access (Article 21). Also noteworthy is that police authorities, seemingly, have no special interest in correcting false information in their hands: communication of the error to the agencies that have sent the false information is subject to not 'imply in a "disproportionate effort"'[180] (which will almost invariably be the case if data circulate around the world), and, in any case, the police are never liable if they are 'not responsible',[181] which apparently includes any negligence on their part.

The debate about limitations to the principle of availability within and outside the EU

When we discussed the draft document prepared by the Commission containing general rules on the availability principle, we observed that there was a distinctive lack of enthusiasm for it in the law enforcement community, which seems to be more than happy with all the more specific initiatives already existing and forthcoming. Article 23 of the 2000 Convention on Mutual Assistance in Criminal Matters offers a nice illustration of those initiatives. We saw above how, for the first time, very modest data protection limitations had been imposed on the judiciary in its cross-border work. The 2000 Convention imposes almost no limitation as to the finality of the data exchange, and use of data for offences other than the initial offences, for example, is not prohibited. The regulatory framework is stricter for police work: in this sense, Article 39 1990 Schengen Convention prescribes that use of data for other purposes is not allowed unless there is authorisation from the transmitting member state.

Many member states are unwilling to add further limitations along the lines of Schengen to the work of the judiciary. On the contrary, the principle of availability invites them to remove all limitations: by virtue of the principle, any police or justice official of one member state may automatically access data held by its colleagues in another member state. If this was already very clear in

the original 2005 proposal drafted by the Commission, with the explicit aim to abolish all limitations, thus opening the way to 'interoperability of national databases or direct (online) access',[182] it more concretely gave way to a multitude of case-specific articles and permissions for transfers of police data even to private parties.[183] Following the intervention of the MDG, the situation appears even more threatening: now, only two Articles cater for the whole principle of availability: one for availability among member states and one for availability to third countries.

As far as availability among member states is concerned, the framework decision only states that its general principles shall apply to data transmitted by one member state to another.[184] Given the battered data protection principles (for instance, the finality principle as enhanced by the 'further processing' notion, or the police approach to information accuracy), the principle of availability will amount to nothing less than complete and total freedom for every state agency to process police and similar personal data within the EU.

The situation regarding international police data transfers is even more problematic, as the EU cannot allow the member states to have too many differences in approach. Under the 1995 Data Protection Directive, all transfers of data from the EU to third countries are conditional on a series of requirements,[185] with a final say for EU institutions that can overrule member state decisions. For example, if the Commission determines that a third country does not offer 'adequate' protection, the member states must comply with its decision.[186]

The October 2005 Commission proposal set up a directive-like system, allowing some central control over the third countries to which national law enforcement agencies would send data. However, the MDG seems to have moved away from this idea, preferring to leave the task of taking 'adequacy' decisions to member states.[187] Additionally, the bilateral agreements of member states are expressly not affected by the framework decision, which could ultimately lead to the probably 'unprofessional' situation whereby, for instance, Belgium may deem that Nigeria provides 'adequate' protection, and thus exports its police records there, while, at the same time, France thinks otherwise and prohibits such exports. In this example, a major problem could arise if Belgium acquires data from France under the principle of availability and wishes to send the data to Nigeria. For this type of situation, the MDG seems to have accepted as a last resort that

> *the competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.*[188]

Altogether, the model is feeble and cannot be compared to the stronger central control of the first pillar, whereby data transfers are ultimately less harmful to individuals, representing yet another example of the reduction of individual rights under the framework decision.

The framework decision and other police cooperation instruments (Schengen, Europol, etc)

We commented above on the fragmentary character of European data protection, as all police cooperation instruments have established their own data protection controls and agencies (the Schengen JSA, the Europol JSB, the Eurojust JSA and the CIS JSA). With the exception of the Eurojust Joint Supervisory Authority, all these agencies are actually composed of almost the same representatives,[189] who are generally the same people who participate in the Article 29 Working Party to discuss matters related to the first pillar as representatives of their own national supervisory authorities. Those representatives, nevertheless, do not have an institutionally recognised forum allowing them to meet and discuss at EU level data protection in the third pillar in general. To solve this problem, the European Data Protection Commissioners met on 14 September 2004 in Wroclaw, Poland and adopted a resolution to set up a 'joint EU forum on data protection in police and judicial cooperation matters (data protection in the Third Pillar)'. The resolution highlights the contrast between the first pillar, where the Article 29 Working Party is in place, and the third pillar, where there is no equivalent body; the three joint supervisory bodies covering Europol, Schengen and Eurojust have specific mandates and, according to the resolution, 'a broader approach is required to secure a uniform level of data protection safeguards for the whole area of police and judicial cooperation'.[190]

An obvious aim of the original 2005 draft proposal was to affect as little as possible other, already existing police cooperation instruments (Schengen – including the SIS II – Europol, Eurojust, etc)[191] and, indeed, the proposed framework decision did not replace those specific regulations. In the same spirit, there was also no question of merging the different JSAs. Instead, the proposal chose to establish a Working Party, in a way parallel to the Article 29 Working Group, allowing the representatives of the existing JSAs to meet and together play a consultancy role on matters related to the third pillar.

The creation of a parallel group to the Article 29 Working Group for the third pillar would, indeed, fill a gap in the institutional role of data protection commissioners. However, it could be only part of the answer, as the opinions of the Article 29 Working Party tend to be simply ignored by the Council and Commission; and even the European Parliament, whose reports do take notice of the Working Party's opinions, has, until now, routinely ignored its views on third pillar issues. Also, this amounts to an extremely complicated model that will probably, in practice, prove rather ineffective for the protection of individual privacy.

The MDG is not very favourably disposed towards this aspect of the 2005 draft proposal and neither is the current German Presidency.

The March 2007 German Presidency's proposal for a Council framework decision

In January 2007, the German Presidency asked the European Commission to prepare a revised proposal.[192] In March 2007, the German Presidency presented its own new draft.[193] Like the Commission's proposal, the Presidency's draft includes general rules on the lawfulness of the processing of personal data, provisions concerning specific forms of processing, rights of the data subject, confidentiality and security of processing, judicial remedies, liability, sanctions, national supervisory authorities, and the transfer to third states. Modifications and amendments are suggested within all chapters of the draft, the most important ones to be mentioned at this point, however, are the following:

- The proposal will now also apply to Europol, Eurojust and the third pillar Customs Information System, whereas authorities or other offices dealing specifically with matters of national security are explicitly excluded from its scope (Article 3 II), though these bodies are not explicitly specified.

- One of the major innovations of the draft is the inclusion of Article 26, which aims to combine the existing data protection supervisory bodies, which have hitherto been established separately for the SIS, Europol, Eurojust, and the third pillar Customs Information System, into a single data protection supervisory authority, merging with it the advisory working party provided for in the earlier draft. However, a separate Council decision will be necessary in order to establish that body. The Presidency intends to submit conclusions to the Council endorsing that aim and asking the Commission to bring forward a

proposal for the relevant Council decision as soon as possible. Having the aim to cover the whole of the third pillar, including Europol, Eurojust and the third pillar Customs Information System, the draft also aims to ensure that more extensive specific data protection rules in the relevant legal instruments remain unaffected. Where the framework decision is to replace existing specific data protection provisions, the data protection framework decision explicitly stipulates this.

- Another far-reaching new clause implements very controversial measures with regard to the exchange of data with third states. First, the proposal reiterates that the framework decision is without prejudice to any obligations and commitments incumbent upon member states or upon the EU by virtue of bilateral and/or multilateral agreements with third states. Furthermore, personal data received from or made available by the competent authority of another member state may be transferred to third states or international bodies only if the competent authority of the member states which transmitted the data has given its consent to transfer in compliance with its national law.

- Finally, in the most recent Article 36 Committee meeting on 22-23 March 2007, the German Presidency also outlined its position with regard to the controversial question about the scope of the proposal, explaining that 'the revised draft Framework Decision had taken into account the work of the MDG on the proposal but that it had decided to restrict the scope of the proposal to the exchange of data between Member States, thus excluding data processing at a domestic level.'[194]

Critical assessment of the framework decision and the position of the German Presidency

Towards the end of 2006, after the Finnish Presidency[195] concluded work on the framework decision and handed it over to the German Presidency, both the EDPS and the European Parliament chose to intervene to alert the Council to the clear compromise of individual rights created by the wording of the text, at least as it was being discussed at that time. The EDPS expressly declared himself to be 'worried about indications that current negotiations in Council are leading to a fragmented and lowered level of protection for the citizens' and thus

> *strongly urge[d] the delegations to reconsider. The EDPS is concerned that legislation aiming at facilitating police and judicial cooperation might be adopted while the legal data protection framework is delayed and diluted.*[196]

In this context, his follow-up opinion focused its criticism mainly on the issue of the scope of the framework decision ('division in data files'), as well as on the treatment of sensitive data, on the possibility of exchanging data with non-law enforcement authorities and private parties, and on international data transfers and the exclusion of the 'adequacy' criterion, as well as on the compromise of fundamental individual rights, such as the right to information.[197]

At the same time, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament submitted a report

> *with a proposal for a European Parliament recommendation to the Council on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,*[198]

produced because the Committee expressly felt

> *extremely concerned at the direction being taken by the debate in the Council, with Member States appearing to be moving towards a data protection agreement based on the lowest common denominator; fearing, moreover, that the level of data protection will be lower than that provided by Directive 95/46/EC and Council of Europe Convention No 108 and that implementation of such an agreement might have a negative impact on the general principle of data protection in each Member State without establishing a satisfactory level of protection at European level.*

It, therefore, identified (admittedly in a similar manner to the EDPS) the framework decision's most problematic areas (sensitive data, finality principle, rights to information and access, the adequacy criterion) and called for maximum participation during the law making process, with representations from national data protection authorities, the Article 29 Working Party and the European Parliament itself, as well as national parliaments.

As Germany took over the EU Presidency from Finland in 2007, a whole new approach saw the light – or rather two new approaches. The first approach

suggested starting again. As mentioned above, on 15 January 2007, it became public that the German Presidency did not want to proceed with discussing the Council draft and had instead asked the European Commission to go back to the drawing board and prepare a 'revised proposal for a Framework Decision on data protection in police and judicial matters'.[199] Although some commentators have interpreted this measure as a promising step for data protection,[200] it is not certain that it was motivated by genuine data protection concerns.[201] As outlined, the German Presidency wishes to change the text drastically in two ways. First, it is of the opinion that the framework decision should be limited to general principles, and, therefore, exist alongside the specific rules in the legal texts concerning Eurojust, Europol, the Customs Information System and Schengen. Secondly, the German Presidency wants to merge the existing third pillar JSAs.

The German Presidency's proposal has just been issued and it is too early to see whether these changes will find any acceptance, as it is also too early to judge the real German willingness to carry through the project of developing a general data protection framework for justice and home affairs. We indicated above that we saw that the project was partly meant to be compensation for a general framework decision regulation of the principle of availability, which, in the meantime, has been taken off the political agenda.

The real intentions of the German Presidency are perhaps best judged by taking into account their second approach, viz, to convince all the EU member states to sign the 2005 Prüm Treaty (discussed above) and to develop first pillar directives and third pillar framework decisions in order to transpose the Prüm Treaty at EU level.[202] As we have seen, the Prüm Treaty provides for a system for exchange of data, such as DNA, vehicle data and fingerprint data, and although it does not mention the 'principle of availability', it does establish a similar principle, the principle of 'exchange of information'. Member states seem to be more than satisfied for the moment with this step-by-step approach to turn the general principle of availability into practice. Although in general terms a progressive approach might appear to be a low bid benefiting data protection,[203] the price for it could be no framework decision on data protection, no European supervision (since Prüm does not foresee it) and no regulation of the many questions and problems surrounding third pillar data processing in general.[204]

Conclusion

Data protection concerns grew out of worries regarding mass data processing by the state back in the 1960s. Laws on data protection were first established on a national level, and were later followed by certain tentative attempts to provide international and European harmonisation. The subsequent decades have brought a significant turn of focus, with private processing now placed in the forefront. This development has been fostered primarily by the fact that personal information acquired a commercial value during the 1980s, as well as by the consistent and repeated policy decisions taken when the 1995 Data Protection Directive 46/95 was released to leave all security-related processing out of its scope. By 2006, commercial processing enjoyed a comprehensive and well tested regulatory scheme while state (security) processing had none. It was then only a matter of time before such discrepancy made itself apparent; in this sense, the international 'terrorism' climate only aggravated an already existing problem that had become institutionally visible with the creation, by the 1992 Maastricht Treaty, of the third pillar structure devoted to justice and home affairs policy-making.

The creation of an area of freedom, security and justice is the most ambitious project of European integration. The current speed of the development of an EU justice and home affairs policy contrasts strongly with the previous modest steps to combat terrorism in the TREVI groups of the 1970s and 1980s, as well as with non-Community efforts like Schengen, and has surprised many spectators. We have already offered an overview of this development: the Schengen acquis was integrated into Union law by the Treaty of Amsterdam in 1999, allowing the databases created under its rules, the SIS and Eurodac, to also come under EU law. Partly prompted by the terrorist attacks in New York and Washington, Madrid and London, numerous initiatives for combating terrorism and serious cross-border crimes, such as the Eurojust decision, the European arrest warrant and many others have been introduced, sometimes even in accelerated procedures. One of the main objectives in the third pillar is now to guarantee smooth, free data exchange and, accordingly, several new initiatives – both inside and outside the EU framework – have been launched to improve the processing and exchange of data in police and judicial cooperation. The SIS II, successor of the SIS I, and the VIS will increase the quantity of data stored by EU institutions; biometric information (now needed for residence permits and visas) has already transformed its nature.

Although it is clear that these developments demand appropriate political and data protection safeguards, discussing data protection in the third pillar

is, however, never easy, since there is no equivalent to the Data Protection Directive in the first pillar. Separate sets of rules have established a series of different actors, with each being responsible for the supervision of different data transfers according to different data protection norms and, furthermore, certain categories of data are stored and exchanged via various information systems (SIS, Eurodac, VIS) falling partly under the first and partly under the third pillar. These systems possess their own regulations and their own supervisory authorities, just as the institutions and bodies clearly falling under the third pillar, such as Europol and Eurojust, also have their own data protection regulations and their own supervisory authorities, even if, additionally, plans are being set up to give them access to some of the other information systems. Finally, the structure of European data protection also includes the European Court of Justice, which disposes of only a minimum of competences when it comes to the third pillar but is often forced to outline the thin line between the first and third pillars with regard to data processing issues.

To sum up, data protection in the EU is today a complex and obscure architecture that can only prove to be a labyrinth for the data subject affected, especially with regard to processing for law enforcement purposes. Still, a lot has already been achieved to improve the protection of data in the field, although it is not always very visible. Lack of European competences to regulate data protection regarding justice and home affairs has been remedied by using the 1981 Council of Europe Data Protection Convention as a reference document and by creating national safeguards and national data protection authorities. Specific data protection provisions regarding Schengen, Europol and (to a lesser degree) Eurojust live up to expectations and foresee a valuable system of annual reporting to the European Parliament by the respective data protection authorities installed within these bodies. Most notably, first pillar competences to regulate data protection have had considerable, if indirect, implications for justice and home affairs processing of data. Indeed, the 1995 EU Data Protection Directive, although not applicable to these forms of processing, has led to national data protection laws with a general scope, including police and justice processing operations, as well as to the obligation to create and finance national operational data protection authorities that have become pivotal actors in the control of national police and judicial authorities and collaborate at the European level to help citizens to control their data. Precisely to enhance this cooperation, the 1995 directive established the previously mentioned 'Article 29 Working Party', a unique data protection lobby established in the heart of the EU, very present in third pillar discussions with its opinions and its advice to the EU institutions, and this even despite its lack of formal powers to intervene.

In addition, the 2001 Regulation No 45/2001 established the also very relevant European Data Protection Officer to supervise the processing of personal data by Community institutions. Although he has no competence to monitor the processing of personal data by bodies established outside the Community framework, he has become an important actor in third pillar data protection organisations, due to his explicit powers regarding certain databases, such as Eurodac, and his general assignment to cooperate with the data protection authorities in the third pillar, as well as his general consultancy role for all matters that could concern data protection in the EU. The data protection advice given by the EDPS to the EU institutions regarding third pillar initiatives can be considered as important as his other achievements.

The proposed framework decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters is supposed to replace all stand-alone agreements for the exchange of third pillar data, regardless of whether they were concluded by single member states or they are EU instruments, or, at least, to constitute a common basis for all similar future agreements to observe. Having said this, it should also be noted that the framework decision should, from the beginning, accommodate all existing obligations until their expiration or amendment, by expressly referring to and acknowledging them. Nevertheless, these provisions should not conceal the framework decision's real objective: to constitute the common basis for all data exchanges within the third pillar, both within and outside the EU; once it is released, all other case-specific legislation (for instance, Schengen, Europol, Eurojust, or bilateral member states' agreements) will have to adhere to its provisions. It is probably the realisation of this central role that the framework decision would hold that led to such strong disputes about its final wording: at the time of writing this contribution, its formulation by the Council and the MDG is unacceptable from a data protection perspective and has raised a series of objections both by the EDPS and the Parliament. However, given the framework decision draft's 'birthmarks', a text with absolutely no regard to almost half a century of data protection in Europe actually came as no surprise: it was born at DG Justice and further developed by the MDG, where the police and the Ministries of Interior are invariably represented, without the participation of any single data protection representative in the whole law making process.

Things seem currently to be standing still, as the MDG has agreed the version of the text under consideration after a year and a half of discussions, the EDPS and the Parliament have rejected it altogether and the German Presidency has obviously not placed it at the top of its agenda. From a data protection

perspective at least, the only sensible way forward, would be to scrap the text altogether and work again on certain necessary improvements on the original proposal of the Commission, this time ensuring institutional data protection representation during the whole process: only in this way will the framework decision become once again a 'data protection text' rather than a 'police cooperation' document.

With these fundamental considerations in mind, and as a whole year has passed since the release of the first draft of the framework decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters, it is undeniable that the final contents and wording of its, admittedly problematic, text will have to be carefully examined when they are finally released. In the meantime, a few assertions may be made. First, a similar instrument appears necessary to us, given the existence of case-specific legislation (Schengen, Eurojust, etc). Although we believe most of these regulations have efficient data protection capacity, they inevitably have to be based on some kind of general text, a text that ought to have preceded them but which is, nevertheless, still welcome. In particular, we see a need for a text addressing specific new technological developments (such as profiling) and new models of policing (such as intelligence-led policing), not addressed in Convention 108 and Recommendation No R (87) 15. Also, there is an urgent need to regulate law enforcement transfers to third countries. Cases such as *Swift* and *PNR* call for a European approach. Since more of these cases are to be expected, this has to be a general one.

Second, it is to be expected that the framework decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters, although it may resemble the Data Protection Directive, will probably offer 'less' data protection than its title implies: its subject-matter (crime prosecution) and timing (the climate of international terrorism) appear to afford a greater level of 'openness' and 'understanding' to police and other crime prosecution-related needs – this might not have been the case ten years ago, but today it certainly configures a reality that cannot be overlooked. In our introduction, we discussed the position taken by the EDPS in 2006, calling for rapid and urgent regulation to balance newly proposed security policies (such as the principle of availability). It seems that the EDPS eventually changed his mind, as in his second opinion on the proposal for a Council framework decision on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters, he wrote:

> *The EDPS recommends that the Council allows more time for the negotiations, so as to achieve a result that offers sufficient protection. Although the EPDS recognises the importance of adopting the Framework Decision by Council in the short term, he warns that the rapidity of the decision making should not lead to a lowering of the standards of protection.*[205]

Cautious pessimism about the sincerity of third pillar law making may explain this remarkable change of position.

Notes

1 For the first author, this publication is partly the result of a project on law, technology, and shifting balances of power, funded by the Dutch Organisation for Scientific Research (NOW). The authors wish to thank Gloria González Fuster (Institute of European Studies, Vrije Universiteit Brussels) for corrections and suggestions.

2 EDPS, 'EU and the right to privacy', *EDPS Newsletter*, no 6, 26 October 2006, pp1-2 (www.edps.europa.eu.).

3 Compare to recital 5 of the 1995 EC Data Protection Directive: 'Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States whereas the exchange of personal data between undertakings in different Member States is set to increase whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market'.

4 Elspeth Guild and Evelien Brouwer, 'The Political Life of Data The ECJ Decision on the PNR Agreement between the EU and the US', *CEPS Policy Brief*, no 109, July 2006, pp9-10.

5 EDPS, 'EU and the right to privacy', loc cit, p2.

6 See, eg, Edward V Long, The intruders: the invasion of privacy by government and industry, New York, Praeger, 1966; Alan F Westin 'Science, Privacy and Freedom: Issues and proposals for the 1970s' Part I 'The current impact of surveillance on privacy' (1966) *66 Col L Rev* 1003 and Part II 'Balancing the conflicting demands of privacy, disclosure and surveillance' (1966) 66 *Col L Rev* 1206; Arthur R Miller, 'Personal privacy in the computer age: the challenge of a new technology in an information-oriented society' (1969) 67 *Mich L Rev* 1091.

7 R Ellger 'Die Entwicklung des Datenschutzes in der Europäischen Union' in: Datenschutz im europäischen Umfeld, Weber, Thürer, Zäch, Zürich 1995; B. Siemen, Datenschutz als europäisches Grundrecht, Berlin, Duncker & Humblot, 2006.

8 D Rowland, 'Data Retention and the War Against Terrorism – A Considered and Proportionate Response?' *The Journal of Information, Law and Technology (JILT)*, 2004 (3), p2 (< http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_3/rowland/>).

9 For a discussion of some of these laws, including the Netherlands, see E-J Koops, R Leenes and P De Hert (eds), Constitutional Rights and New Technologies. A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States, Information Technology & Law Series (IT&Law Series), The Hague, TMC Asser Press, 2007, to be published. On Greece data protection, V Papakonstantinou, Information Technology Law *('Nomika Themata Pliroforikis")*, Sakkoulas Publications, 2005, Athens-Thessaloniki, pp9-190. On British data protection see D Rowland, loc cit, pp2-8.

10 See for an overview of data protection regulations governing employment law, Fr Hendrickx (ed), Employment Privacy Law in the European Union: Human Resources and Sensitive Data, Antwerp, Intersentia, 2003.

11 Fair Credit Reporting Act 1970, 15 USC § 1681 et seq, Senate and House of Representatives of the United States of America in Congress assembled
(available at http://www.ftc.gov/os/statutes/031224fcra.pdf (last accessed 31 August 2006)).

12 Fair Debt Collection Practices Act 1977, 15 USC 1692 et seq. Senate and House of Representatives of the United States of America in Congress assembled. Available at http://www.ftc.gov/os/statutes/fdcpa/fdcpact.htm (last accessed 31 August 2006). For a discussion of existing models of data protection regulation, see *EPIC and Privacy International, Privacy and Human Rights 2005*, an international survey of privacy laws and developments, Washington, Epic org, 2006, pp10-40.

13 For a strong critique, see L Bergkamp, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy', *Computer Law and Security Report*, 2002, vol 18, no 1, pp31-47.

14 See Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview* Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, p89 ff. Available at: hftp://ftp.jrc.es/pub/EURdoc/eur/20823en.pdf (last accessed 24 November 2006); P De Hert, 'European Data Protection and E-Commerce: Trust Enhancing?' in *JEI*, Prins, PMA Ribbers, HCA Van Tilborg, AFL Veth and JGL Van Der Wees (eds), Trust in Electronic Commerce, The Hague, Kluwer Law International, 2002, pp171-230.

15 Council of Europe, Convention for the Protection of Individuals with regard to automatic processing of personal data, 28 January 1981, *ETS* No 108.
Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last accessed 30 August 2006).

16 Art 13: 'The Parties agree to render each other mutual assistance in order to implement this convention. For that purpose each Party shall designate one or more authorities (...).'

17 See for instance Art 6 of the Convention: 'Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions'.

18 Additional protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No18; 18/11/2001), Council of Europe, 1 July 2004.

19 Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) allowing the European Communities to accede, Council of Europe, 15 June 1999.

20 See http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/ (last accessed 30 August 2006).

21 See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=4/25/2006&CL=ENG (last accessed 30 August 2006).

22 The Schengen aquis as referred to in Art 1(2) Council Decision 1999/435/EC of 20 May 1999, OJ L 239 of 22.9.2000.

23 For instance, Recommendation No R (81) 1 on regulations for automated medical data banks (23 January 1981); Recommendation No R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983); Recommendation No R (85) 20 on the protection of personal data used for purposes of direct marketing (25 October 1985); and Recommendation No R (86) 1 on the protection of personal data used for social security purposes (23 January 1986).

24 Recommendation No R (87) 15 regulating the use of personal data in the police sector, Council of Europe, 17 September 1987. Available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1987_15.pdf (last accessed 30 August 2006).
25 An individual shall not be regarded as 'identifiable' if identification requires an unreasonable amount of time, cost and manpower.
26 See principle 2.4 of the recommendation.
27 See on these concepts, P De Hert, W Huisman and Th Vis, 'Intelligence led policing ontleed', [Intelligence led policing critically examined], *Tijdschrift voor Criminologie*, 2005, vol 47, no 4, 365-376; J-P Brodeur, 'High Policing and Low Policing: Remarks about the Policing of Political Activities', *Social Problems*, 1983, vol 30, nr 5, pp507-520; P Gill, Rounding up the usual suspects, Ashgate Publishing Ltd, England, 2000.
28 Principle 2.1 of the recommendation states that: 'The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation'.
29 According to a decision adopted on 7 February 1995 by the Committee of Ministers (see text of Second and Third Evaluation, all available at the Council of Europe internet site, http://www.coe.int).
30 Communication of the Commission to the Council on the Community Policy on Data Protection (Com doc no 73/4300 final), 21 November 1973.
31 *Data Protection, Data Security and Privacy*, Commission of the European Communities, 1977, Luxembourg.
32 Bericht im Namen des Ausschusses für Wirtschaft und Währung über die Mitteilung der Kommission der Europäischen Gemeinschaften an den Rat über die Politik der Gemeinschaft auf dem Gebiet der Datenverarbeitung (Doc 74/153), Europäisches Parlament, 1974.
33 European Parliament Resolution, OJ C 100 of 8.4.1976.
34 Entschließung zum Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung, *Official Journal of the European Union*, 1979, No C 140.
35 Eg, Report on the protection of the rights of the individual, 02.10.1981; European Parliament Resolution of 09.03.1982.
36 Single European Act, OJ L 169 of 29.6.1987.
37 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, OJ L 239 of 22.9.2000, pp13-19.
38 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 gradual abolition of checks at their common borders, OJ L 239 of 22.9.2000, pp19-63.
39 In addition to data protection rules for the SIS, the Convention contains data protection rules that apply to simple telephone conversations between police. See for a detailed discussion: P De Hert and J Vanderborght, Informatieve politiesamenwerking over de grenzen heen [Cross-border exchange of police data], Brussels, Uitgeverij Politeia nv, 1996.
40 Art 115.1 Schengen Convention.
41 Note that Art 39 Convention provides for police information exchange on request, but does not oblige member states to reply. See P De Hert, 'Trends in European police and judicial cooperation with regard to data exchange', *Panopticon, Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, 2004, vol 25, no 1, (26-56), p38. Available at: http://www.panopticon-net.org/.

42 This view is, legally speaking, incorrect, but it is clear that Art 39 Schengen Convention comes closer to what could be seen as a genuine legal basis for international exchange of data by the police compared to the Interpol text, which has no status of international public law.
43 Compare EDPS, Opinion of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final*)*, OJ C 116 of 17.5.2006, pp8-17.
44 Treaty of Prüm, 27 May 2005. Available at:
http://www.statewatch.org/news/2005/jul/schengenIII-german-full.pdf (last accessed 30 August 2006).
45 Apart from the seven original signatory states (Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain), another four states (Finland, Italy, Portugal, Slovenia) have declared their intention to accede to the Treaty. The Treaty is expected to be in force in the original signatory states in the first half of 2007 at the latest. The ratification processes in the countries intending to accede to the Treaty are also well advanced.
See http://www.statewatch.org/news/2007/jan/dresden-prum.pdf (consulted February 2007).
46 Arts 20-22 Prüm Treaty.
47 Arts 17-19 Prüm Treaty.
48 Art 23 Prüm Treaty. See also Art 27 that is Schengen-related (cooperation on demand).
49 Art 24 Prüm Treaty.
50 Art 26 Prüm Treaty.
51 Art 16 Prüm Treaty.
52 Arts 1-15 Prüm Treaty.
53 Art 34 Prüm Treaty.
54 See Art 2, para 2, Arts 5 and 8 Prüm Treaty.
55 Thierry Balzacq, Didier Bigo, Sergio Carrera and Elspeth Guild (2006), 'Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats', 2006, *Ceps Working Paper* no 234, available at: www.ceps.be.
56 'An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'
57 In this sense, Hijmans has noted that the Article 29 Working Party has come to see itself as 'the independent EU Advisory Body on Data Protection and Privacy' (H Hijmans, 'The European Data Protection Supervisor: the Institutions of the EC controlled by an independent authority', *Common Market Law Review* 43, 2006, pp1313-1342).
58 There are some tensions between the national data protection authorities on the one hand and the EDPS on the other hand. These tensions will not be discussed here. Obviously the EDPS, being a new body (infra) still has to find his place, but this will probably be a question of time.
59 Regulation (EC) No 45/2001 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, OJ L 8 of 12.1. 2001.
60 As included in the Annual Reports of the EDPS over 2004 and 2005.
Available at: www.edps.europa.eu.
61 H Hijmans, 'The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority', *Common Market Law Review*, 2006, vol 43, pp1313–1342, at p1120 with reference to Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM (2004) 835 final. And the three Proposals regarding the Second Generation Schengen Information System (SIS II), (COM (2005) 230 final, COM (2005) 236 final and COM 2005) 237 final.

62 As included in the Annual Reports of the EDPS over 2004 and 2005.
Available at: www.edps.europa.eu.
63 Title IV Maastricht Treaty is often described as the 'third pillar' of the EU, after the Treaty provisions on the European Communities ('first pillar') and the Common Foreign and Security Policy ('second pillar'). The second and third pillars are still based in general on intergovernmental cooperation rather than the 'Community method' of law-making and judicial control.
64 Protocol of 2 October 1997 on the integration of the Schengen acquis into the framework of the European Union. See also on the acquis, OJ L 239 of 22.9.2000, pp19-473.
65 J Schutte, 'Unification and Harmonisation of Criminal Procedures in the European Union', in J Nijboer and W Sprangers (eds), Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunities for International Standards, Amsterdam, Thela Thesis, 2000, pp43-55; P De Hert, 'Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs', in J Apap (ed), Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement, Cheltenham (UK), Edward Elgar Publishing Limited, 2004, pp55-102. It should also be noted that first pillar measures, in case of conflict with other legal rules, take precedence over such other rules. The notion of direct effect, according to which individuals may invoke Community legislation before national courts if it is clear, precise and unconditional, has been developed by the case-law of the ECJ, primarily in the context of the Community legal system. See, in particular, *Van Gend en Loos* judgment, C-26/62 [1963] ECR 1. In the framework of the third pillar, it is interesting to mention the recent judgment of the ECJ delivered on 16 June 2005, Case C-105/03, *Maria Pupino*. In the context of the interpretation of the framework decision on the standing of victims in criminal proceedings, OJ L 82/1 of 22.3.2001, the ECJ has confirmed that the principle that national law must be interpreted in conformity with Community law also applies in the third pillar. By urging national courts to read domestic law in such a way as to conform to the provisions of framework decisions, the ECJ ensures that these instruments will be given some effect, despite the absence of proper domestic implementation. The ECJ has, therefore, also introduced the notion of indirect effect into the third pillar. See José Castillo Garcia, 'The power of the European Community to impose criminal penalties', *Eipascope*, 2005/3, 27-34 with reference to M Wasmeier and N Thwaites, 'The battle of the pillars: does the European Community have the power to approximate national criminal laws?' *European Law Review*, 2004, vol 29, no 5, October, pp610-620.
66 J Peek, 'International police cooperation within justified political and judicial frameworks: Five theses on TREVI' in J Monar and R Morgan (eds), The third pillar of the European Union, Brussels, European Interuniversity Press, 1994, pp201-207.
67 The 1998 Tampere Programme comprised legislative, administrative, and institutional measures, envisaging new institutions such as Eurojust, and the European Police College.
68 M Den Boer, '9/11 and the Europeanisation of anti-terrorism policy: A critical assessment', *Notre Europe,* 2003, Policy Papers no 6, http://www.notre-europe.asso.fr/IMG/pdf/Policypaper6.pdf; M den Boer and J Monar, '11 September and the challenge of global terrorism to the EU as a security actor', *Journal of Common Market Studies,* 2003, vol 40, pp11-28; C Fijnaut, 'The attacks on 11 September 2001, and the immediate response of the European Union and the United States', in C Fijnaut, J Wouters, and F Naert (eds), Legal instruments in the fight against international terrorism: A transatlantic dialogue, Leiden, The Netherlands, Martinus Nijhoff, 2004, pp15–36; J Wouters, 'The European Union and September 11', *Indiana International & Comparative Law Review,* 2003, vol 13, pp719-775; K L Scheppele, 'Other people's PATRIOT acts: Europe's response to September 11', *Loyola Law Review,* 2004, vol 50, pp89-148; J Monar, 'The problems of balance in EU Justice and Home Affairs and the impact of 11 September', in M Anderson and J Apap (eds), Police and justice co-operation and the new European borders, The Hague, Kluwer Law International, 2002, pp165-182; S Peers, 'EU responses to terrorism', *International and Comparative Law Quarterly,* 2003, vol 52, pp227-244.

69 European Council, EU Presidency Conclusions, 4-5 November 2004, Annex I: *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, Brussels, 13 December 2004, Council doc no 16054/04, OJ C 198 of 12.8.2005, p22.
70 Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, OJ C 198 of 12.8.2005, p1.
71 European Commission, Press Releases, 12 October 2005. Available at:
http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/
367&format=HTML&aged=0&language=EN&guiLanguage=en (last accessed 31 August 2006).
72 See doc no 5239/06 for the database statistics as of 1 January 2006; the document can be consulted at the public register of Council documents http://register.consilium.eu.int.
73 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, OJ L 69 of 15.3.2005.
74 Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 162 of 30.4.2004.
75 Member states supply the SIS through national networks (N-SIS) that are connected to a central system (C-SIS). This is supplemented by a network known as SIRENE (Supplementary Information Request at the National Entry), which is made up of representatives from the national and local police, customs and the judiciary. SIRENE will be replaced by a new communications system called SISNET, which will eventually become a 'European Information System' that also contains data on immigration.
76 Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190 of 18.7.2002.
77 Common Position on the exchange of information on stolen and lost passports between the 'SIS countries' and Interpol, 24 January 2005.
78 Regulation (EC) No 1160/2005 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, OJ L 181 of 13.7.2005.
79 P De Hert, 'Trends in European police and judicial cooperation with regard to data exchange', loc cit, p40.
80 It is unclear whether the proposals to modify the duration of the alert will get through. It was at any rate one of the proposals made during the negotiations.
81 OJ L 381 of 28.12.2006, p4.
82 Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Europol Convention).
Available at: http://www.europol.eu.int/index.asp?page=legalconv, last consulted 24 August 2006. See T Schalken, 'On Joint Investigation Teams, Europol and Supervision of Their Joint Actions' *European Journal of Crime, Criminal Law and Criminal Justice*, 2002, vol 10, no 2, pp70-82.
83 Numerous amendments to the Europol Convention have been adopted, amending its scope of action and its competencies.
84 P De Hert, 'Les banques de données d'Europol', *Vigiles. Revue de droit de police*, 1996, no 3, pp36-44.
85 Art 24.1 Europol Convention. See on this body: http://europoljsb.ue.eu.int/.
86 Although there seems to be no limitation on the kind of data that Europol can process (non-suspected persons and sensitive information), there are good checks and balances on this, including provisions that distinguish between hard and soft data and provisions that shield

sensitive information from member states that have no particular concern in a certain case that only involves some member states.

87 J D Occhipinti, 'The politics of EU police cooperation: Toward a European FBI?' Boulder, CO: Lynne Rienner, 2003.

88 Operational agreements signed: Bulgaria, Canada, Croatia (not yet ratified), Iceland, Norway, Romania, Switzerland, USA, FBI, United States Secret Service, Eurojust and Interpol. Operational agreement in progress: Albania, Australia, Bosnia Herzegovina, FYROM, Israel, Moldova, Monaco, Serbia and Montenegro and Ukraine.

89 Strategic agreements signed: Colombia, Russian Federation, Turkey, EU Commission, ECB, EMCDDA, OLAF, UNODC and WCO.

90 See Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM (2005) 475 final, 4 October 2005 (henceforth, Original Council Proposal), p2.

91 V Mitsilegas, 'The New EU–USA cooperation on extradition, mutual legal assistance and the exchange of police data', *European Foreign Affairs Review,* 2003, vol 8, pp515-536.

92 Council of the European Union, Council Decision of 28 February 2002 setting up Eurojust with a view to reinforce the fight against serious crime, 2002/187/JHA, OJ L 63 of 6.3.2002, pp1-13.

93 In 2005, the Council approved the Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, OJ C 68 of 19.3. 2005.

94 H Brulin, 'La protection des données: quête et errements dans le troisième pilier', in *Actualités du Droit Pénal Européen*, 9, La Charte, Brussels, 2003, p149.

95 P De Hert and FM Tadic, 'The Prosecuting Officers Enter the Play. About Eurojust and the European Judicial Network', *Strafblad. Het nieuwe tijdschrift voor strafrecht*, 2003, vol 1, no 1, pp43-70.

96 Commission of the European Communities, Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005) 597 final, Brussels, 24 November 2005.

97 COM (2005) 597 final, p7.

98 COM (2005) 597 final, p7.

99 COM (2005) 597 final, p5.

100 COM (2005) 597 final, p5.

101 COM (2005) 597 final, p8.

102 EDPS, 'Comments on the Communication of the Commission on interoperability of European databases', Brussels, 10 March 2006. Available at: http://www.edps.eu.int/; P De Hert and S Gutwirth, 'Interoperability of police databases within the EU: An accountable political choice?' *International Review of Law, Computers & Technology*, vol 20, no 1-2, March-July 2006, pp21-35.

103 EDPS-European Data Protection Supervisor (2006a), Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), Brussels, 28 February 2006. Available at: http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf.

104 The communication seems to be written by someone within the Commission who has taken stock of all the existing databases and simply dreams of taking command of them all for no reason of general interest.

105 Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213 of 15.6.2004.

106 See P De Hert, W Schreurs and E Brouwer, 'Machine-readable identity documents with biometric data in the EU. Overview of the legal framework', loc cit, pp5-7.

107 Guidelines for the introduction of a common system for an exchange of visa data, adopted by the JHA Council on 13 June 2002. Council Document 9615/02 VISA 92 COMIX 386.
108 P De Hert, 'Trends in European police and judicial cooperation with regard to data exchange', loc cit, p46.
109 Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas COM (2004) 835 final. Available at:
http://eur-lex.europa.eu/LexUriServ/site/en/com/2004/com2004_0835en01.pdf (last accessed 31 August 2006).
110 Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, 14359/06, Interinstitutional File: 2004/0287 (COD), 25.10.2006.
111 'EU: Fingerprinting of children - the debate goes on', *Statewatch News Online*, 2006 (http://www.statewatch.org/news/2006/aug/02eu-fingerprinting-children.htm). See also EDPS, 'Opinion on the European Commission proposal for amending the Common Consular Instructions in view of the implementation of the Visa Information System (VIS)' 27 October 2006, via www.edps.europa.eu.
112 Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, COM (2005) 600 final.
113 Draft Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, 14359/06, Interinstitutional File: 2004/0287 (COD), 25.10.2006.
114 Commission Decision of 3 November 2006 establishing the sites for the Visa Information System during the development phase, OJ L 305/13 of 4.11.2006.
115 COM (2005) 597 final, p6.
116 Idem, p10.
117 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197 (12.07.2005), pp3-23.
118 Art 23 para 3 adds: 'In the circumstances of the particular case, the communicating Member State may require the Member State to which the personal data have been transferred to give information on the use made of the data'.
119 Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol, OJ L27 of 24.1.2005.
120 For an analysis, see M Deflem, 'Wild beasts without nationality: The uncertain origins of Interpol, 1898–1910' in P Reichel (ed), The handbook of transnational crime and justice, Thousand Oaks, CA, Sage, 2005, pp275–285; M Deflem, Policing world society: Historical foundations of international police cooperation, Oxford, New York, Oxford University Press, 2002; P De Hert and J Vanderborght, Informatieve politiesamenwerking over de grenzen heen *[Cross-border exchange of police data]*, Brussels, Uitgeverij Politeia, 1996.
121 Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts, Kingdom of Sweden, 4 June 2004. Available at: http://register.consilium.eu.int/pdf/en/04/st10/st10215.en04.pdf (last accessed 30 August 2006).
122 Information and intelligence: any type of existing information or data, appraised, processed and analysed or not, that could be used in a crime investigation or a criminal intelligence operation to detect, prevent or investigate a crime or a criminal activity. Such information or

intelligence includes: (a) information and intelligence in records or files kept by competent law enforcement authorities; (b) information kept in records or files by other authorities, to which competent law enforcement authorities have access, either directly or indirectly; (c) information on holders, ex-directory and listed respectively, of telephone, cellphone, telex, fax, e-mail or website subscriptions or addresses kept by telecom operators; (d) information on persons and freight kept by transport companies; (e) any other information or intelligence or data, appraised, processed and analysed or not, that has been obtained within the framework of a criminal investigation or a criminal intelligence operation or that may be obtained without the use of coercive powers.

123 'Access to data by law enforcement agencies', *Statewatch*, 2004, May-July, vol 14, no 3/4.

124 Regulation 2252/2004 on biometric features in EU passports, COM (2005) 0010 final, 13 December 2004. Available at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0010:EN:NOT (last accessed 30 August 2006).

125 Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322 of 9.12.2005.

126 Council Framework Decision 2005/876/JHA of 21 November 2005 on the organisation and content of the exchange of information extracted from criminal records between Member States, OJ L 322 of 9.12.2005.

127 'France Germany and Spain to share access to databases', *Statewatch*, 2004, May-July, vol 13, no 3-4.

128 *Heise-online*, Internationales Strafregister-Netz läuft im Echtbetrieb. Available at:
http://www.heise.de/newsticker/meldung/73926 (last accessed 31 August 2006).

129 Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final, p12, October 2005.
Available at: http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/554.pdf (last accessed 30 August 2006).

130 Undertakings of the Department of Homeland Security (DHS) Bureau of Customs and Border Protection, section 15. However, the interpretation by the Department of Homeland Security of the agreement leaves one with the impression that it will keep data for longer: 'Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. […] [Q]uestions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions'. (Council doc no 13738/06, Letter to the Council Presidency and the Commission from the Department of Homeland Security of the United States of America.)

131 'EU: The principle of availability takes over from the notion of privacy: what price data protection?' *Statewatch Bulletin*, 2004, vol 14 no 6, November-December 2004, pp1-2.

132 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 available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 of 13.4.2006.

133 Peter Van de Velde, 'EU finally adopts its long-debated Data Retention Directive', 24 May 2006. Available at:
http://www.twobirds.com/english/publications/articles/EU_adopts_Data_Retention_Directive.cfm (last accessed 23 November 2006).

134 It does not apply to the content of electronic communications: no data revealing the content of a communication may be retained.

135 The exact categories of data to be retained are listed in Art 5 Data Retention Directive.

136 Initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, 28 April 2004, CRIMORG 36, Council doc no 8958/04.
137 D Cronin, 'MEPs to accept data retention', 10 November 2005, available at: http://www.europeanvoice.com/archive/article.asp?id=24044.
138 Article 29 Data Protection Working Party, 'Opinion on Directive 2006/24/EC on the retention of data', available at:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf
139 See EDRI, 'Final push for single EP vote on data retention', loc cit, p1.
140 See EDRI, 'Polish plans for 15 years mandatory data retention', *EDRI-gram: biweekly newsletter about digital civil rights in Europe*, 5 December 2005, no 3.24, pp3-4.
141 EDRI, 'EDRI and PI call on EP to reject data retention', *EDRI-gram: biweekly newsletter about digital civil rights in Europe*, 5 December 2005, no 3.24, p3.
142 D Rowland, loc cit, p15.
143 *Ireland v the Council and the European Parliament* (Case C-301/06), via curia.europa.eu.
144 Case C-301-06, *Ireland v Council and Parliament*, asking for annulment of Directive 2006/24/EC on Data Protection.
145 European Court of Justice, judgment of the Court of 31 January 2006 in Case C-503/03 (*Commission v Spain*).
146 European Court of Justice, judgment of the Court of 31 January 2006 in Case C-503/03 (*Commission v Spain*), para 35.
147 European Court of Justice, judgment of the Court of 31 January 2006 in Case C-503/03 (*Commission v Spain*), para 53.
148 European Court of Justice, judgment of the Court of 31 January 2006 in Case C-503/03 (*Commission v Spain*), para 55.
149 Comp A Van Bossuyt, 'Vrij verkeer van personen heeft voorrang op Schengen', *De Juristenkrant*, 8 March 2006, no 125, pp1 and 13.
150 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 (notified under doc no C (2004) 1914), OJ L 235 of 6.7.2004, pp11-22.
151 Council Decision 2004/496/EC on the conclusion of an agreement between the European Community and the US on the processing and transfer of PNR ('Passenger Name Records') data, OJ L 183 of 20.5.2004, pp83-85.
152 European Court of Justice, judgment of the Court of Justice of 30 May 2006 in *European Parliament v Council of the European Union* and *European Parliament v Commission of the European Communities*, Joined Cases C-317/04 and C-318/04, OJ C 178/2 (29.07.2006).
153 L Creyf and P Van de Velde, 'PNR (Passenger Name Records): EU and US reach interim agreement', *Bird & Bird Privacy & Data Protection Update*, October 2006, no 11–
(http://www.twobirds.com/english/publications/newsletters/). On 3 July 2006, the Council and the Commission notified termination of the agreement with effect from 30 September 2006. On 7 September 2006, the European Parliament adopted a report in which it asked the Council to negotiate – under the Parliament's oversight – an interim agreement, whereby the Parliament wanted to ensure that the US offered adequate protection of the passenger data collected and which should provide for a change to the 'push' system (under which US authorities must request specific data which will then be selected and transferred) instead of the present 'pull' system (whereby access is granted to the full database and airline passengers data are directly

accessed online by the authorities concerned). In its report, the Parliament further requested joint decision-making rights over the negotiation of the final agreement with the US. On 6 October 2006, shortly after the Court-set deadline of 30 September, EU negotiators reached an interim agreement with their US counterparts. The conflict of laws situation that has existed since 1 October 2006 thereby appears to be, at least temporarily, solved. The interim agreement would ensure a similar level of protection of the PNR data as before and it would also comply with the US request that the PNR data can be more easily distributed between different US agencies. A move from the 'pull' system to the 'push' system should be undertaken at a later date. The nature of PNR data available to US agencies remains unchanged. The interim agreement will apply from its date of signature, which is due to be completed by 18 October, and will expire no later than 31 July 2007. By this date a new (superseding) agreement should be reached between the parties who meet again in November 2006 to begin discussions on that point.

154 In this light, the PNR judgment contrasts with the more liberal approach of the ECJ in its earlier judgment in the *Österreichischer Rundfunk* case (see above).

155 B De Schutter and P De Hert, 'La Belgique est-elle prête pour appliquer la loi sur la vie privée dans le domaine policier', *Vigiles. Revue de droit de police*, 1995/3, pp1-12.

156 'The transfer of data to the USA concerning air passengers clearly shows that the distinction between the First and Third Pillars is becoming ever finer and that a horizontal approach needs to be adopted to examine rights and freedoms' (Franco Frattini, *Data protection in the area of Justice, Freedom and Security*, speech held at a meeting with the Joint Supervisory Authorities under the Third Pillar; Brussels, 21 December 2004 (SPEECH/04/549), p5. Available via: http://europoljsb.ue.eu.int (consulted February 2007)).

157 The Council of the European Union (then 15 governments) set up a working party on data protection in the 'third pillar' in May 1998. The 'Action Plan of the Council and the Commission on how best to implement the provisions of Amsterdam establishing an area of freedom, security and justice' (13844/98) said that data protection issues in the 'third pillar' should be: 'developed within a two year period' (IV.47(a)). Not until August 2000 was a draft resolution drawn up by the Working Party. This was revised five times, the last being on 12 April 2001 under the Swedish Presidency of the EU (6316/2/01) when agreement appeared to have been reached and the Article 36 Committee was asked to address outstanding reservations. From this point on there has been silence – and the Working Party was abolished in 2001 when the Council was restructured to 'streamline' decision-making.

158 Declaration adopted by the European Data Protection Authorities in London on 2 November 2006. Available at: http://www.edps.europa.eu/legislation/06-11-02_London_declaration_EN.pdf (last accessed 26 November 2006).

159 Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM (2005) 475 final, 4 October 2005 (henceforth, Original Council Proposal), p2.

160 Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM (2005) 475 final, 4 October 2005.

161 See the documents referred to in http://www.statewatch.org/eu-dp.htm.

162 Council of the European Union, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).

163 In November 2006 the EDPS issued a second critical opinion and in December 2006 the European Parliament adopted a report saying that it intended to re-examine the issue as the Council had ignored its views. See European Data Protection Supervisor Second Opinion and respective Press Release of 29.11.2006 ('EDPS warns Council not to lower EU citizen's rights

in third pillar data protection'), as well as the European Parliament's Recommendation to the Council on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2006/2286(INI)). Also Tony Bunyan, 'EU data protection in police and judicial cooperation matters: Rights of suspects and defendants under attack by law enforcement demands', *Statewatch*, 2006. Available at: http://www.statewatch.org/news/2006/oct/eu-dp.pdf (last accessed 22 November 2006).

164 One commentator has observed that their 'primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects'. See Lord Avebury, Speech to the Joint Parliamentary Meeting on EU developments in the area of freedom, security and justice at the European Parliament on October 3. Available at: http://www.statewatch.org/eu-dp.htm. Suggestions by member states for the establishment of an ad hoc group for the processing of the framework decision, where data protection authorities (either national or the EDPS) would also participate, were rejected ('Monitoring the state and civil liberties in the UK and Europe, EU policy "putsch": Data protection handed to the DG for "law, order and security"', *Statewatch,* March-April 2005, vol 15 no 2). The only institutional data protection participation in the law-making process included one single presentation by the EDPS of his office's respective opinion in the MDG.

165 See p4, point 7 in Presidency Note for discussion at the Article 36 Committee on 25-26 January: EU doc no 5435/07.

166 5435/07 CRIMORG 12 DROIPEN 4 ENFOPOL 5 DATAPROTECT 3 ENFOCUSTOM 9 COMIX 57.

167 Presidency, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters *(*7315/07; 13.03.2007).

168 See Original Council Proposal, p4. The Commission, regardless of the fact that a different Directorate General released Directive 95/46, felt that the framework decision 'should not hamper consistency with the general policy of the Union in the area of privacy and data protection on the basis of the EU Charter for Fundamental Rights and of Directive 95/46/EC. The fundamental principles of data protection apply to data processing in the first and in the third pillar'.

169 The Commission proposal does not abolish the provisions of those legislative instruments that are affected by it (Schengen, Europol, Eurojust, Customs Information System), but contains general provisions for similar processing; at the same time the said instruments shall continue to apply as sector-specific legislation, governing their particular subject matter. Although the proposed framework decision does not take into consideration conflicts of law, the understanding of the drafters is that should the proposed framework decision be released, those provisions of the said instruments that directly contradict the provisions of the proposed framework decision shall become null and void (not necessarily by means of direct mention in the text of the framework decision, but rather by adequate application of the lex specialis criterion upon them).

170 'Information from a Communication of the Council to the Article 36 Committee (Coreper) on "Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters – Questions on scope"', 13918/13.10.2006. Available at: http://www.statewatch.org/eu-dp.htm. Also, 'Data protection proposal in a muddle – member states divided – three Council working parties discussing the draft measure', *Statewatch,* 2006, (available at: http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm).

171 Information from doc no 13918/13.10.2006,
(available at http://www.statewatch.org/eu-dp.htm) of the Council (see above).

172 See Art 5 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
173 Elspeth Guild and Evelien Brouwer, loc cit, p5.
174 See Art 4 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
175 See Art 22 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
176 See Art 28 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
177 See Art 7 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
178 See Art 6 of the Original Council Proposal.
179 See Art 6 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
180 See Art 22 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
181 See Art 28 of Council doc no 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).
182 See Original Council Proposal, p3.
183 See Arts 11-15 of the Original Council Proposal.
184 Several member states think that this is the only use of the framework decision (see above).
185 See Art 25 Directive 95/46/EC. Member states must allow the transfers only if the third country in question provides what can be considered to be an '*adequate*' level of protection unless the transfer falls under one of the derogations established in Art 26.1 of Directive 95/46/EC (unambiguous consent of the data subject, implementation of contractual or pre-contractual measures, protection of vital interests, etc) or it is accompanied by appropriate contractual clauses (Art 26.2 Directive 95/46/EC).
186 See Art 25.4 and Art 25.6 Directive 95/46/EC. For an overview of countries with an adequate protection regime, see also:
http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.
187 See Art 15 of Council doc no 13246/13.11.2006 (available at:
http://www.statewatch.org/eu-dp.htm).
188 See Art 15(c) of Council doc no 13246/13.11.2006 (available at:
http://www.statewatch.org/eu-dp.htm).
189 'Indeed it is common for the same person to sit on all three JSAs under a different hat (applying different rules)' (The European Union Committee, 'European Union – Fifth Report', Ordered by the House of Lords to be printed 22 February 2005, http://www.publications.parliament.uk/pa/ld200405/ldselect/ldeucom/53/5302.htm).
190 Resolution to set up a 'joint EU forum on data protection in police and judicial cooperation matters' (data protection in the third pillar) adopted on 14 September 2004 by the European Data Protection Commissioners meeting in Wroclaw, Poland. According to this network of representatives of national data protection supervisory authorities, 'There is no alternative to creating a high and harmonized data protection standard in the EU Third Pillar' (see: 'Declaration adopted by the European Data Protection Authorities', London, 2 November 2006). See also B De Schutter, 'Van Schengen naar Prüm. Bedenkingen over privacybescherming in Europese strafrechtelijke samenwerking', in J Christiaens, E Enhus, A Nuytiens, S Snacken, P Van Calster (eds), Criminologie: tussen kritiek en realisme. Liber Amicorum Christian Eliaerts, Brussels, Vubpress, 2007, pp143-154.

191 See preamble (20) and Chapter VIII of the Council's Original Proposal where only specific provisions seem to be affected by the framework decision, rather than all of its principles expressly superseding any other provisions of the same subject-matter.
192 See Point 7 of the Presidency doc no 5435/07, 18 January 2007
(available at http://www.statewatch.org/news/2007/jan/eu-dp-jan-07-5435-07.pdf).
193 Presidency, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (7315/07, 13.03.2007).
194 Statewatch, 'Observatory on data protection in the EU'
(available at: http://www.statewatch.org/eu-dp.htm).
195 In order to properly set the time scene, it should be noted that the Finnish Presidency, just one month before these EDPS and Parliament's interventions on the framework decision, had also concluded the interim PNR Agreement (see above), that also raised heated disputes with regard to its level of data protection (which disputes the Parliament expressly adopted, see for instance the respective debate at the Parliament's website, http://europarl.europa.eu, Ref. 20060901IPR10254).
196 See EDPS respective Press Release of 29 November 2006
(available at: http://www.edps.eu.int).
197 See EDPS, 'Second Opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters', 29 November 2006 (available at: http://www.edps.eu.int).
198 European Parliament, Session doc no A6-0456/2006 FINAL, December 11, 2006.
199 'EU: Informal Justice and Home Affairs Minister meeting, Dresden, Germany, 14-16 January 2007', *Statewatch News Online*, 15 January 2007 (02/07), sub 1 (http://www.statewatch.org) with reference to p4, point 7 in Presidency Note for discussion at the Article 36 Committee on 25-26 January: EU doc no 5435/07.
200 'It has to be hoped that the Commission when revising the proposal takes into account the views of the European Data Protection Supervisor and the European Parliament and not just those of the Council. When it does return to the table the Council must give it to the Working Party on Data Protection and not to the working party comprised of law enforcement officials who have proved quite incapable of balancing their demands with the rights of citizens to meaningful data protection' (T Bunyan, quoted in 'EU: Data protection: German Presidency to ask for "revised" proposal', *Statewatch News Online*, 26 January 2007 (03/07), sub 2 (http://www.statewatch.org)). Moreover, the German Presidency wants no central European control of the adequacy of third countries with which member states exchange data.
201 The German Presidency shares most of the views taken by the member states against the initial Commission Proposal. The Presidency does not want any further limitations of the possibilities to exchange data by the judiciary and wants to stick to the flexible regulations foreseen in Art 23 2000 Convention on Mutual Assistance in Criminal Matters.
202 'EU: Prüm Confusion', *Statewatch News Online*, 26 January 2007 (03/07), sub 5 (http://www.statewatch.org) and 'EU: Two draft Council Decisions to transpose parts of the Prüm Treaty into EU law', *Statewatch News Online*, 26 January 2007 (03/07), sub 8 (http://www.statewatch.org).
203 We saw that the Prüm exchange of data is based on the idea that identifiable data is not exchanged as a rule. It is only when there is a match of non-identifiable data that an exchange of identifiable data follows.
204 In his comment on the proposed framework decision on data protection in the third pillar, the EDPS observes that neither the proposed framework decision, nor the proposal for a Council framework decision on the exchange of information under the availability principle address the sensitivity and specificities of biometric data and DNA profiles from a data protection point of view. This good suggestion is followed by some general recommendations: 'The

EDPS recommends that specific safeguards should be provided, in particular with a view to guarantee that: biometric data and DNA profiles are used only on the basis of well established and interoperable technical standards, their level of accuracy is carefully taken into account and might be challenged by the data subject through readily available means, and that the respect of the dignity of persons is fully ensured.' (EDPS, Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 final, 19 December 2005), www.edps.europa.eu, § 80.

205 EDPS, 'Second Opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters', 29 November, 2006, p7 (available at: http://www.edps.eu.int).