1. International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

Paul de Hert and Bart de Schutter

I. Introduction

A. What data protection is all about

As a result of the rapid development in computer technology, large amounts of information relating to individuals (‘personal data’) are routinely collected and used by public administrations and in every sector of business. Since the 1970s, several EU Member States have passed data protection legislation, that is, legislation protecting the fundamental rights of individuals and in particular their right to privacy, including inter alia protection from abuse resulting from the processing (i.e., the collection, use, storage, etc.) of personal data. In general, these laws specify a series of rights for individuals and demand good data management practices on the part of the entities that process data (‘data controllers’).

These basic practices or principles are also spelled out in the international legal data protection texts produced by institutions such as the United Nations, the Organisation for Economic Cooperation and Development (OECD), the Council of Europe, and the European Union. Each of these organisations produced what has become a classic basic data protection instrument, respectively the Guidelines on data protection, the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, the Convention for the protection of individuals with regard to automatic processing of personal data, and the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data.

1. The authors wish to thank Gloria González Fuster (Institute of European Studies, Vrije Universiteit Brussels) for corrections and suggestions.

The ideas behind these legal instruments on data protection are similar. They all try to more or less reconcile fundamental but conflicting values such as privacy, free flow of information, governmental need for surveillance and taxation, etc. More concrete data protection takes the form of a set of principles governing the processing of personal data, whether in public or private sectors. Whenever there is processing of such data, the data protection principles apply. These principles are: 1. the collection limitation principle; 2. the data quality principle; 3. the purpose specification principle; 4. the use limitation principle; 5. the

11. There should be limits to the collection of personal data and any such information should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
12. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.
13. The purposes for which personal data are collected should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
14. Personal data should not be disclosed, made available or otherwise used for purposes other than those first specified except: a) with the consent of the data subject; or b) by the authority of the law.
International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

Data protection is, however, still not internationally acknowledged as a global issue. There is no world treaty on data protection and many countries have no formal recognition of the need to protect personal data. The 1980 OECD Guidelines and the 1990 UN Guidelines are important at the global level, but they lack legally binding force. The OECD text is also less detailed compared to the European documents, being just a short document containing no more than a listing of the data protection principles. The mentioned European legal instruments widened the scope of 1980 OECD Guidelines in many respects and established the need for independent supervisory data protection authorities, which are unknown in the OECD Guidelines.

It is interesting to note that Europe has now developed two basic texts with regard to data protection. The approach of the Council of Europe Convention can be labelled ‘guideline-oriented’, whereas the EU rules are rather formalistic and bureaucratic in nature. Different reasons have been suggested to explain this difference in approach between the two European documents. The Directive came into place almost fifteen years after the Convention. In the meantime, data protection doctrine developed considerably. Almost all EU Member States (with the exception of Italy and Greece) had legislation in place based on the Convention. The Directive consequently benefited from all the practical experience accumulated in those years. The Convention and the Directive have a different nature and are part of different legal systems. While the Convention has a non-executive character and should be viewed in the framework of Public

15. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
16. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
17. An individual should have the right of notification, access and rectification.
18. A data controller should be accountable for complying with measures that give effect to the data protection principles.
International Law, the Directive can impose much more specific obligations on the member states of the Union, which are then, under European Law, obliged to implement its provisions into national law.

Data protection is thus about controlling the actors processing personal data of citizens and this control is either done by the data subjects themselves or, in Europe at least, by data protection supervisory authorities. Controlling national actors is of course much easier than controlling actors outside the legal regime of the Member State of the data subjects.

B. Objectives and outline of this contribution

In spite of increased attention to issues of data protection in the last 20 years, most citizens are still largely unaware of the extent to which their personal data are processed by police and judicial authorities. The reality, however, is that police and judicial databases are full of sensitive information, and one could consider all police data on persons to be sensitive. In fact, depending on the context, the sheer fact that someone appears in a police database may already be considered as sensitive information. Even fewer citizens are aware that their personal data are being transmitted by Member States to other Member States and to third countries outside the EU.

The naivety of citizens regarding their presence in police databases may well play into the hands of those who favour (new) security policies that infringe on fundamental rights. Adequate data protection rules, on the level of the Member States and on the European level, contribute to the protection of fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law, as well as in the 2000 Charter of Fundamental Rights of the European Union.

In this contribution we look at the EU rules governing the processing of data in the field of Justice and Home Affairs (JHA), in particular with

21. With regard to the “non-executive character” of the Convention: The ECHR has been considered as one of the most (if not the most) powerful human rights instruments also because the respect of its provisions is guaranteed by the authoritative rulings of the European Court (e.g., see Jack Donnelly, International Human Rights: A Regime Analysis, 40 [1986] International Organization, pp. 599-642

22. EDPS, ‘EU and the right to privacy’, EDPS Newsletter, no. 6, 26 October 2006, 1-2 (www.edps.europa.eu.).
regard to data transfers to third countries. A fundamental distinction when it comes to protecting individual privacy within the EU ought to be made between the so-called First Pillar and Third Pillar (or JHA) processing. The latter category covers all crime-related and security-related processing of personal information. First Pillar processing normally covers all commercial processing of personal information. Whereas for First Pillar processing Directive 95/46/EC provides a common denominator for data protection, for Third Pillar processing such a common standard does not exist: instead, a patchwork of data protection regulations covers different sector-specific processing (the Schengen Agreement, SIS II, Europol, Eurojust and, recently, the Prüm Treaty). In the present paper we discuss briefly the EU regulatory framework on data protection and the choice between a comprehensive model of regulation and a sectoral or piece-meal approach, as is the case for the Third Pillar in its current state (section II).

Then we proceed with a basic question about the need for an EU approach with regard to transfers of personal data to third countries: Is a European regulation of transfers of data to third countries necessary? (Section III). After discussing this question in the context of the First Pillar (section III A), we will discuss the question in a subsequent paragraph with regard to Third Pillar processing (sections III B to E). We contend that the current data protection patchwork in the Third Pillar is not wholly satisfactory with regard to the issue of controlling transfers of data to third countries. We illustrate this with Europol, the PNR case and the Swift case. The latter PNR and Swift examples show that not all aspects of Third Pillar processing are covered by the current EU framework, as important aspects are delegated to the legal regimes of the different Member States. The Europol example shows us that the EU is in need of a general standard setting with regard to international transfers, complementing the current piece-meal approach.

Subsequently, this contribution will briefly outline the draft framework decision that was forwarded by the Commission to the Council in December 2005 (section IV). Finally, a summary and some concluding remarks will be in section V.
II. The EU regulatory framework on data protection


When pursuing its internal market objective at the beginning of the 1990s, the European Commission launched a package of measures for data protection. The core of these measures was a draft proposal for a Directive on the protection of personal data aiming at establishing the same level of protection within all Member States. In 1995, after five years of discussions, the first and major instrument for data protection was established on 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). This First Pillar instrument regulates the processing of personal data (defined as any information relating to an identified or identifiable natural person) by laying down guidelines determining when the processing is lawful, and prohibiting the processing of special categories of data (e.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life). The Directive specifies the information to be given to the data subjects and their rights, 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. Member States are asked to ensure that one or more public authorities (supervisory authorities) monitor the application within their territory of the provisions adopted pursuant to the Directive.

In the logic of Directive 95/46/EC, the transfer of personal data between EU states is put on equal footing with transfer of data within one legal...

25. “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”.
26. We will come back below to the system of control set up with regard to transfers of data to Third Countries.
The Data Protection Directive applies throughout the EU, irrespective of whether the individuals concerned by the processing are EU citizens or not. The right to privacy of citizens has, as a result of the Directive, equivalent protection across the Union and at the same time, the Directive ensures that companies and other organizations will be able to transfer personal data throughout the EU. Jurisdiction also covers the EEA countries. Subjects wishing to control the use of their data in other Member States can call for assistance to their national data protection authority, which will call upon its colleagues to carry out the control. A similar logic was already built into Article 12 of the 1981 Council of Europe Convention. The second paragraph of this provision states that parties “shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party”.

Directive 95/46/EC was complemented by Regulation (EC) No 45/2001, which provides for criteria with regard to the lawfulness of processing personal data, the transfer of personal data within or between Community institutions or bodies, transfer of personal data to recipients other than Community institutions and bodies, but subject to Directive 95/46/EC, and transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC. Like the 1995 Directive, the regulation defines ‘personal data’ and special categories of processing and provides all kinds of data regulations guidelines, e.g. on information to be given to the data subject. Nevertheless, the Community institutions and bodies can restrict the application of certain articles where the restriction constitutes, among other foreseen exemptions, a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences.

27. Cf. Directive 95/46/EC, Recital 3 “Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded”. Cf. also Recital 9 “Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy (…)”.

Regulation (EC) No 45/2001 also established the European Data Protection Supervisor (EDPS), making him responsible for monitoring the application of its provisions to all processing operations carried out by a Community institution or body. Besides, each Community institution and Community body must appoint at least one person as data protection officer to cooperate with the European Data Protection Supervisor and in particular to inform him of certain sensitive data processing operations. The European Data Protection Supervisor is also requested to cooperate with the national supervisory authorities established under Directive 95/46/EC. According to his mission statement, the EDPS has three sets of tasks: supervision (monitoring), consultation and cooperation.


According to its Article 3 (2), Directive 95/46/EC does not apply to the processing of personal data in the field of JHA. 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 of the Treaty of the European Union. Like Directive 95/46/EC, Regulation (EC) No 45/2001 does not apply to activities falling completely within the scope of the Third Pillar, nor do its provisions apply to bodies fully established outside the Community framework. With regard to activities of the institutions under the Third Pillar, the European Data Protection Supervisor 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 needed.

However, both the Data Protection Directive and Regulation (EC) No 45/2001 do have an impact on the processing in the field of JHA. In this sense, it can be mentioned that, after 1995, the Directive caused a wave of reform of the then existing data protection laws in the Member States and, in most cases, that the reforms were of a general nature, affecting data protection principles that apply to all processing, including processing carried out by police and the judiciary. One can therefore assume that, as a result of the

---

International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

Directive, differences between legal provisions of the Member States were reduced, including differences with regard to processing in the field of justice and home affairs.

Moreover, the Directive established a European Group of data protection Commissioners in its Article 29 of Directive 95/46/EC and this European Group is known as the “Article 29 Working Party”. This unique data protection lobby is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, as well as of a representative of the Commission. The independent advisory body examines any question covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures, and advises the Commission on any proposed amendment of the Directive, as well as on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms. Therefore, the Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community. The Article 29 Working Party has played an important role not only at Community level, but also regarding Third Pillar issues. Indeed, although originally established by a First Pillar instrument and as a First Pillar body, the Article 29 Working Party has tended to position itself as the watchdog of EU data protection in general – especially until the establishment of the European Data Protection Supervisor in 2004. Moreover, it has established close cooperation with the EDPS, which is a full member of the Working Party, as well as with the Joint Supervisory Authority under the Schengen Convention. It has intervened and drawn world attention to crucial data protection issues with Third Pillar relevance such as the PNR-case (infra) and the Swift case (infra) and has advised the European Parliament with regard to data retention regulation (infra).

31. Article 30 of Directive 95/46/EC.
32. In this sense, HIJMANS has noted that the Art. 29 WP 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”, 43 [2006] Common Market Law Review, p. 1313.
33. 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) has still to find his place, but this will probably be a question of time.
Justice, Liberty, Security: New Challenges for EU External Relations

Even though we noted that the EDPS is in general terms not competent to supervise the processing of data performed in the context of the third pillar, 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 the supervision of the Central Unit of Eurodac (Article 20 of the 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. In addition, Article 46(f)(ii) of 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, 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 the so called PNR case (see below). Indeed, the Court explicitly referred to Article 41(2) of 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.

C. Data protection in the field of JHA: the current state

The foregoing may not blind us to the current general state of affairs. Whilst for First Pillar processing the EU legislative framework, together with some forty years of legislative history in some EU states (Germany, France, Sweden), has led to a well-regulated and clearly-defined processing environment for all commercial processing of personal information, unfortunately this is not the case with Third Pillar processing. The Data Protection Directive expressly excluded such processing from its scope (see above) and, although some EU Member States saw it fit to regulate such processing through their own national Data Protection Acts, this by no means constitutes the norm. Quite to the contrary, apart from a Council Convention of 1981 and a couple of Recommendations, the field is left basically unregulated. The EU Third Pillar patchwork is supplemented with the national rules on data protection in the field of JHA, but these rules are only consistent up to a certain degree (with very little attention to the problem of transfers to third countries). Criticism concerning this situation has lately become more pronounced.

In this sense, during the public seminar on transatlantic data transfers held at the European Parliament in March 2007\textsuperscript{37}, Yves Poullet expressed his concern regarding the absence of uniform data protection standards throughout all three pillars.\textsuperscript{38} Peter Hustinx, the current EDPS, noted at the same seminar that the lack of the trans-pillar common framework creates problems during negotiations with third countries on, e.g., PNR agreements.\textsuperscript{39} Indeed, the present situation raises the issue of a double standard with regard to, for instance, the US authorities, who are asked to respect the information privacy of Europeans in their anti-terrorist


campaign, whereas the European institutions themselves do not necessarily follow those standards.\textsuperscript{40}

It could be argued that the current Third Pillar situation is extremely problematic. Rather than proceeding rationally, by first establishing the general principles, the institutions and the definitions, and then entering into case-specific legislation (as has been the case within the First Pillar), the EU has already introduced case-specific regulations (Schengen, Europol, Eurojust) while still lacking any standard-setting piece of legislation. One could respond to this argument that a piece-meal approach has the advantage of depth and insight. Indeed, the Schengen Agreement, but also Europol and Eurojust Agreements, all include detailed data protection rules and processes in their own texts, very much along the lines of the Directive, but skillfully adapted to their specific purposes. A major drawback of this approach is that it requires that new legislation be introduced with each new technology or new processing operation, with the result that protection frequently lags behind.

We cannot discuss at great length this choice between a comprehensive model of regulation and a sectoral or piece-meal approach. Let us simply observe that both in the United States and the EU there seems to be a development towards a middle position, by using sectoral laws to complement comprehensive legislation with more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records. The Third Pillar situation contrasts with this. What we are effectively faced with today is a series of sectors that are well-regulated by means of their own texts of reference (Schengen, Europol, Eurojust), but without a uniform basis that would set the standards (e.g. definitions, administrative system, principles) when it comes to police and judicial processing of personal information, in the way that the Directive 95/46/EC performs this task for commercial communications.

Some important standard setting took place in the 1981 Council of Europe Convention and Council of Europe Recommendation No R(87) of 17 September 1987 concerning the use of personal data in the police

\textsuperscript{40} Although it can be pointed out that the US authorities tend to use this argument of “double-standards” repeatedly, and also declared that EU applied “double-standards” in First Pillar matters while negotiating the Safe Harbor Agreement, because some breaches to the Data Protection Directive were believed to take place in the EU territory.
sector, but there may be reasons to question the accuracy of these documents for today’s EU needs. One realizes that this discussion would take us far away from our subject matter. We certainly do not agree with those who say that there is currently a loophole in the EU data protection system, but it must be clear that there is reason to doubt the coherence and clarity of this system.

III. The need for a European regulatory framework on data transfers to third countries

Before drawing any conclusions, we return to our central topic and take one step back by asking one very basic question about the need for an EU approach with regard to transfers of personal data to third countries: Is a European regulation of data transfers to third countries necessary? Having discussed this question in the context of the First Pillar in the next paragraph (sub-section A), we shall discuss it in subsequent paragraphs with regard to Third Pillar processing (sub-sections B to D).

A. Centralised or de-centralised regulatory models for transfers of data to Third States and the choice of the Directive

The question whether a European regulation of data transfers to third countries is necessary was raised in the early nineties with regard to the First Pillar and is raised again today with regard to the Third Pillar. The choice is between letting Member States decide for themselves about protecting data transferred to Third States and creating European supervision of these transfers. Both options have their merit. The first option could be called the model of decentralized decision-making, i.e. the adoption of policies at the level of the EU Member States without any attempt at coordination. One can defend this model claiming that it will produce the most adequate results, as this decentralized approach may prevent bureaucracy and ensure a better fit between the kind of regulation involved and the specific local conditions, thus contributing to overall efficiency.

The second option is the one followed in Directive 95/46/EC. The Directive requires Member States to permit transfers of personal data only to countries outside the EU where there is adequate protection for such data.\footnote{Article 25, Directive 95/46/EC.} The ‘adequacy’ criterion constitutes typical regulatory “gunboat
diplomacy”, which was by no means invented in the EU. The USA, for instance, has implemented the same approach in the case of the Semiconductor Chip Protection Act 1984. It is however the EU that applied this criterion in the data protection field in its relationships with third countries. According to the Data Protection Directive, “the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection” (Art. 25.1). Article 25 also contains the procedure to determine whether there is an adequate regime.\footnote{Cf. Article 25, paragraph 2, Directive 95/46/EC. Pursuant to this provision, the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on Protection of Individuals with regard to the Processing of Personal Data has issued guidelines to facilitate the assessment: WP 4 (5020/97), First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy, a discussion document adopted by the Working Party on June 26, 1997; WP 7 (5057/97) Working document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?, adopted by the Working Party on January 14, 1998; WP 9 (5005/98) Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries, adopted by the Working Party on April 22, 1998; WP 12: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, adopted by the Working Party on July 24, 1998, available at the website europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12/en.} It is striking that the Commission, and not the Member States, has the last say in the procedure, although the participation of a ‘comitology’ committee was incorporated in the decision-making process to reinforce control by national authorities.\footnote{Cf. Article 31, Directive 95/46/EC.}

When there is no adequate protection, transfers may only take place in circumstances specified in Article 26. This will be the case, for example, if:

- an individual has given his unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract (e.g., employment contracts) or for the implementation of pre-contractual measures taken in response to his/her request (e.g., application for a job);
International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

- the transfer is necessary or legally required for the establishment, exercise, or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the individual (e.g., transfer of medical data concerning an individual hospitalised in a non-EU country).

Other exceptions are provided by the Directive and show that, even for data flows to those countries that do not ensure an adequate level of protection there are a great many bridges and doors. For some of these doors, the individual holds the key. However, the existence of exceptions is not enough to re-assure business. For the fact is that even in the best-case scenario a number of non-EU countries fall short of an adequate level of protection, and individuals may be reluctant to give their consent to the transfer to such countries of their personal data.

The Data Protection Directive pays due attention to this reality. Another door remains open even if the above conditions are not met, and this time the key to the door are held by the industry itself. Companies operating worldwide may indeed wish to establish safeguards that make them less dependent on the good will of the legislators in a given country. Article 26 (second paragraph) recognises that adequate safeguards may be provided by the company itself and that these safeguards may in particular result from appropriate contractual clauses. When there is no adequate protection and the exemptions in Article 26 do not apply, the transfer must be forbidden (‘blocked’).

However, this radical step, possibly causing disruption to international data flows and commercial transactions, is not the general rule. Not only are there many exceptions and is there the possibility to adopt contractual clauses, but there is also a complex procedure concerning the possible decision to block: Member States must inform the Commission, which will start a Community procedure to ensure that any Member State decision to block a particular transfer is either extended to the EU as a whole or reversed. Moreover, Article 25(4) of the Directive states that decisions to

44. As shown above, the Directive applies to transfers of data that take place in the course of direct contacts with individual consumers on the Internet. It might be argued that an individual transferring his own data has given his consent to such a transfer; one of the exemptions in Article 25 allowed by Article 26, provided that such an individual is properly informed about the risks involved. Cf. http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm, November 3, 1998.


46. The Committee and the Working Party assist the Commission in this task.
block transfers are taken on specific individual cases. This implies that a
decision to block a transfer would only apply to other transfers of the same
type, not to all transfers to the country concerned. Everything in the
Directive is designed to keep the scope of blocking decisions as narrow as
possible.

B. The adequacy principle and the idea of a safe data protection
harbour

The Directive requires all personal data transferred to countries outside the
Union to benefit from ‘adequate protection’. Transfers of personal data to
countries outside the EU where there is adequate protection for such data
cannot be blocked. The Data Protection Directive only prevents transfers
of personal data to third countries where the level of data protection is
considered ‘inadequate’.

It must be pointed out that the European approach to the ‘adequacy’
requirement is not very strict and does not demand as high a level of
protection as ensured under the First Pillar. As Poullet explains, according
to the “Methodology Paper” adopted by the Article 29 Working Group in
1998, the concept of “adequate protection” has to be distinguished from
other concepts like “equivalent protection” or “sufficient protection”.
According to the paper: "With the adequate protection requirement, the
question to be solved is …: considering the specific privacy risks linked
with a TBDF and taking into consideration the number and quality of the
data transferred, the types of usages pursued by the transfer, the eventual
onward transfers, etc., can we consider that the Data Protection of the data
subjects is or not effectively ensured following the main requirements of
the EU directive." 47 Therefore, Poullet characterises the European
approach to the standard of adequate protection as pragmatic, relying on

The overall policy of the Commission is to negotiate with countries that
have a questionable reputation for data protection. The case of the US is
well known. Because US data protection is non-statutory and there is no
independent data protection authority, it is regarded as inadequate by
definition. Yet, blocking the transfer of business data to the USA was widely
considered to be unthinkable. Therefore, the European Commission
adopted, on 26 July 2000, a decision on the adequacy of the level of data

47. Y. Poullet, above note 37, 8.
48. Y. Poullet, above note 37, 8-9.
International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

protection in the US with the EU Data Protection Directive. The decision, containing the Safe Harbour principles, entered into force on 1 November 2000. The Commission decision specifies the conditions for an adequate level of protection in the US concerning the transfer of data from the European Community to the United States. By agreeing to the Safe Harbour principles, US business will therefore be able to collect data and transfer personal data between the US and the EU Member States. In this way, US organisations can keep in line with the European data protection principles, create trust and confidence, and develop best business practice.

This construction is intended only for the US (and applies only to data transmitted from the EU to the US, and not vice versa). Major US business concerns, such as Microsoft, have accepted the principles, thereby allowing the transfer of personal data across the Atlantic. The software giant also goes a step further and uses the EU standards as a basis for its information transfers around the globe. This voluntary extension may be interpreted as an indication of the potential of the Safe Harbour principles for international acceptance.

C. The adequacy principle in the field of JHA?

The rule regarding transfers to third countries in the First Pillar is clear: 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. The question that needs to be addressed here is whether that rule should apply also in the Third Pillar. Against that position one could


50. It is stipulated that US companies should comply with seven basic principles. Notably, they must inform customers and employees about why they collect and use information. Companies also must offer consumers the option to choose not to have their personal information disclosed (opt-out policy). Finally, companies must allow consumers or employees to access information collected about them so that they can correct, amend, or delete it. Important for what will follow is the provision in the Safe Harbour document stating that "Where, in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts".

51. For the principles, see: www.export.gov/safeHarbour/.

52. See 'Microsoft to adopt EU’s data privacy rules’, Financial Times, www.qlinks.net/items/qitem10661.htm.
argue that law enforcement is of public interest, which in many cases deserves priority treatment over privacy considerations. One could add that law enforcement authorities are to be trusted to protect data as part of their duty to uphold professional secrecy; that these authorities only demand data on a case-by-case basis and that the judiciary especially is committed to a strong regulatory framework limiting the possible use of data received. Reference could be made to the fact that Interpol, the world’s largest international police organization with 186 member countries, is working on the basis of self-imposed data protection principles. Of course, one could object that Interpol, like Europol (see below) is not illustrative of a model of decentralized decision-making, but rather underpins the usefulness of a channelled approach with some supervision. Perhaps a better illustration of the decentralized model is given by the rules governing the exchange of data between judicial authorities. This kind of exchange 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, 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

53. Created in 1923, this organisation that has no formal legal basis in a convention, facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. Interpol aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. Interpol’s constitution prohibits ‘any intervention or activities of a political, military, religious or racial character.’ For more than a decade this organisation, partly under pressure of host country France, has self-imposed data protection rules: On Rules adopted by the General Assembly at its 72nd session (Benidorm, Spain, 2003) in Resolution AG-2003-RES-04. Entered into force on 1 January 2004; Rules amended by Resolution AG-20054-RES-15 adopted by the General Assembly at its 74th session (Berlin, Germany, 2005), see http://www.interpol.com/public/icpo/default.asp. On Interpol, see P. De Hert & J. Vanderborght, Informatieve politie samenwerking over de grenzen heen [Cross-border exchange of police data], Brussels, Uitgeverij Politeia nv., 1996, 635p.


they are very flexible and are clearly not intended to limit the work of the judiciary. 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.67

There is, as we can see, however, no requirement of adequacy. This requirement is certainly lacking in the many bilateral agreements on mutual assistance in criminal matters between the individual Member States and third countries. These agreements, which sometimes go back to the nineteenth century, traditionally ignore data protection principles and focus on more conventional principles of international criminal law, such as the principle of reciprocity and speciality. Moreover, the presence of an international agreement is not always mandatory, and some Member States engage in mutual assistance in criminal matters with third countries solely on basis of their national law and without any formal legal international or bilateral basis.

The foregoing shows that international cooperation in the field of JHA has functioned without requirement of adequacy and sometimes without data protection rules at all, and continues to do so. A requirement of adequacy in the field of JHA was, however, created with the 2001 Additional Protocol to the 1981 Council of Europe Convention.67 The main purpose of this Protocol is to improve the application of the principles contained in the Convention by adding two substantial new provisions, one on supervisory authorities and one supplementing Article 12 of the Convention on transfer of data across national borders:68 “Each Party shall provide for the

---

65. Article 23 paragraph 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”.


68. A. Blas, l.c., 7-8.
transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer” (Additional Protocol, Article 2.1).

All the implications of this requirement in the Protocol are not immediately clear. What is its relationship with the bilateral agreements Member States have concluded with regard to mutual assistance in criminal matters with countries without data protection or adequate data protection? Can the EU, not being bound as such by the 1981 Council of Europe Convention, pursue a policy encouraging transfers to third countries in disrespect of the adequacy requirement? Is there a liability issue when the EU contributes to actions of Member States that disrespect this requirement? The examples of Europol, PNR and the Swift case may provide an answer to these questions.

D. Arguments in favour of the adequacy principle in JHA

1. Europol

The Europol Convention,59 which formally established Europol, entered into force on 1 October 1998. Europol’s tasks as they were defined were 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 that concerned them, and of any connections between criminal offences; to aid investigations in the Member States by forwarding all relevant information to the National Units; and to maintain a computerized system of collected information. Europol’s data collection utilizes mainly three systems: an automatic information system, a work files system and an index system.60 The information system contains all available data about persons suspected of or convicted for offences within Europol’s mandate (Article 8 [1] Europol Convention). The work files refer to data about persons as mentioned in Article 8 (1) Europol


International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

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 acting within the framework of its national legislation, and Europol when collecting, processing and utilizing personal data, must take all necessary measures to ensure a standard that corresponds at least to the standard resulting from the implementation of the principles of the Council of Europe's 1981 Convention, and so doing, must take account of Recommendation No R(87) of 17 September 1987 concerning the use of personal data in the police sector. Each Member State must appoint a national supervisory body to independently monitor, and in accordance with its national law, the permissibility of the input, the retrieval and any communication to Europol of all personal data by the Member State concerned; it must also examine whether the rights of the data subject have not been violated. An independent joint supervisory body, the Europol Joint Supervisory Body, is 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 utilization of the data held by Europol. This 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 personal data have been collected, stored, processed and utilized by Europol is lawful and accurate.

In order to widen the exchange of information, Europol has over the years concluded numerous operational agreements (including the exchange of personal data) and strategic agreements (not including the exchange of personal data) with several third countries and organizations. The latter agreements, which are less interesting from a policing 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 taken the initiative to solve the data protection issue of international data transfers in the Third Pillar. On what basis does Europol distinguish between states with which operational agreements are concluded and states with which

61. Article 24.1 of Europol Convention. See on this body: http://europoljsb.ue.eu.int/
62. 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 & Montenegro and Ukraine.
63. Strategic agreements signed: Colombia, Russian Federation, Turkey, EU Commission, ECB, EMCDDA, OLAF, UNODC and WCO.
(only) strategic agreements are concluded? This is a relevant question, since the list of operational agreements is certainly too long from a data protection perspective. Given the lack of any provisions of general application, Europol has initiated exchanges with third countries that have not even been included in the list of countries that provide an ‘adequate’ level of protection according to the terminology and standards of the First Pillar (Directive 95/46). Moreover, the actual agreements that Europol has concluded are not satisfactory in terms of the protection of individual privacy (see, for instance, the agreement with the USA, and its inexplicably broad Articles 7 or 5).

The foregoing shows that Europol has developed a system of self-regulation regarding international data transfers which though not wholly exempt from criticism constitutes an acceptable alternative in the light of the vacuum in which the organisation has to work and given the political pressure exercised on the organisation to cooperate with U.S. law enforcement agencies. Still, the situation is far from ideal since it puts the organisation in a delicate position.

Data protection provisions in the Europol Convention are impressively elaborate, and the overall image of how the Europol Joint Supervisory Body operates is rather positive. It might be that from a police perspective the existing rules are too strict, a situation that produces counter-productive results. There are signals for instance that Europol may be turning down requests by Member States to transfer data to third countries, while ignoring further action taken by these Member States. Rumour has it that if a Member State wants to transfer data via Europol to countries without data protection, say Nigeria, Europol will refuse to intervene and re-orient the case back to the Member State that took the initial initiative, with the message that it will have to consider the transfer based on its national legislation (which is quite often less strict in comparison with Europol). The Member State will then have to judge the legitimacy of the transfer in the light of its own regulations. This (possible) interplay between the European and the national level, which could eventually lead to forum shopping by police forces, is again far from ideal as far as data protection is concerned.

It should be said that the whole issue regarding Europol and data protection can be considered to be currently in a transitional phase, mainly for three reasons. Firstly, the so-called Third Protocol to the Europol

International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

Convention, signed in 2003, has just entered into force.\textsuperscript{65} It foresees a series of amendments to the Europol Convention, concerning inter alia the possibility of allowing data transfers to third bodies that do not ensure adequate levels of data protection.\textsuperscript{66}

Secondly, with a view to changing the legal basis for the existence of Europol, the European Commission presented, on 20 December 2006, a proposal for a Council Decision establishing Europol, which should substitute the Convention.\textsuperscript{67} Article 24 of the proposal allows communication of personal data to third bodies when deemed necessary for police purposes, and when ‘the Union has concluded an international agreement with the third country, the international organisation or the third body concerned, which permits the communication of such data on the basis of an assessment of the existence of an adequate level of data protection ensured by that body’. The Union, and not Europol, will hence decide whether transfers can be allowed. It is uncertain whether this part of the proposal will be maintained. At a public hearing in the European Parliament,\textsuperscript{68} it was said that Member States were opposed to this provision, without further explanation. At the same hearing, Europol officials observed that the new procedure would be more time consuming. Clearly, the law enforcement community has its reasons for opposing the proposals. However, from a data protection perspective, there is also reason for some criticism. Even if the proposal includes a provision allowing the Union to conclude international agreements with third bodies in which the assessment of an adequate level of data protection has been ensured, the foreseen assessment does not even require consultation of representatives of EU data protection authorities, and the adequacy criterion can suffer exemptions that do not even need to be communicated to those authorities.\textsuperscript{69} Moreover, the proposal substantially modifies the general rules of decision-making for Europol – a change that has an impact

\textsuperscript{66.} Amending therefore Article 18 of the Europol Convention.
also on the conclusion of data transfer agreements and that has not been unanimously welcomed.70

Thirdly, it has to be underlined that some of the provisions referring to data protection in the Europol legal instruments, notably those referring to international data transfers, might eventually contradict provisions in the currently discussed draft Proposal for a Framework Decision on data protection in police and judicial cooperation. Though the applicability of the draft proposal to Europol was originally not even envisaged, it now seems very probable, which raises the question of the relation between its provisions and Europol-specific provisions, particularly where international data transfers are concerned. It is indeed unclear which provisions would be applicable if contradictions occurred.

2. The PNR Case

Since January 2003, European airlines flying into the United States are obliged to provide the U.S. 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’). In accordance with U.S. laws adopted following the terrorist attacks of 9/11, airline companies have 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 up to 34 fields of data, including not only names and addresses, but also contact details such as telephone numbers, email addresses, information about bank numbers and credit cards, and also about meals ordered for flights. The U.S. demand to access data held by European firms for billing purposes without passengers consenting to the transfer or without a proper legal basis for the transfer clearly violates European data protection regulations. The European Commission tried to solve the problem by negotiating with the U.S. officials a series of requirements, and later adopting a decision on adequacy based on Article 25 of the EC Directive on data protection,71 the adoption of which meant that the Commission was convinced that the US would

International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

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\textsuperscript{72} to officially allow the transfers.\textsuperscript{73}

Obviously, the most difficult problem during the negotiations was the one related to the ‘adequacy’ criterion. Because the ‘adequacy’ of the suggested US processing of PNR data on European citizens had not yet been assessed, the Commission attempted to solve this problem as follows: it suggested to Council and Parliament that it would first issue a Decision incorporating an assessment of the US (CBP) processing in relation to the provisions of the Directive (‘Adequacy Finding’), and that it would then enter an international agreement to deal with problems that would not be addressed by this Adequacy Finding – that is, the PNR Agreement. On February 23, 2004, the Council authorized the Commission to negotiate such an agreement with the USA and issued a series of negotiating guidelines. Accordingly, on March 17, 2004 the Commission made its final proposal to the Council so that the latter could issue a Decision “on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection”.

The first PNR Agreement was signed on May 28, 2004 in Washington. The Commission had previously issued its Decision “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”, and the Council had issued its own Decision, “on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection" [idem]. ‘Adequacy’ is guaranteed through a series of Undertakings by the US,\textsuperscript{74} which constitute an integral part of the First PNR Agreement.


\textsuperscript{73} From a US perspective, the new instrument was intended to build upon the Aviation and Transportation Security Act of 2001.

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, the European Court of Justice, on 30 May 2006, annulled Council Decision 2004/496/EC and Commission Decision 2004/535/EC, 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 conclude 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 concerned data transfers fell within a framework established by the public authorities related to public security.

The Court judgement has been regarded as a failure for the European Parliament, which 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 disproportional transfer of data to the United States without proper data protection guarantees. This issue was simply not addressed by the Court.

76. L. Creyf & P. Van de Velde, ‘PNR (Passenger Name Records): EU and US reach interim agreement’, Bird & Bird Privacy & Data Protection Update, October 2006, no. 11, 2p. (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 wants to ensure that the US offers 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 U.S. On 6 October 2006, shortly after the Court-set deadline of 30 September, EU negotiators reached an interim agreement with their U.S. counterparts. The conflict of laws situation that 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.
which concentrated instead on the institutional arguments raised by the European Parliament. Even from this point of view, however, it is doubtful whether the outcome was really what the European Parliament was aiming for, since the result of the judgement was that any new agreement would have to be negotiated in the context of the Third Pillar, where the Parliament has less voice than in the First Pillar, and so it finds itself left out of the picture. Moreover, in the Third Pillar there is only limited control by the European Court of Justice, as its jurisdiction over these matters depends on whether each Member State has made a declaration allowing its national courts to refer questions to the European Court of Justice on Third Pillar issues. Finally, there is the rejection of the 1995 Data Protection Directive as a proper legal basis. On the one hand, the European Court of Justice concluded that the collection of PNR data by the airlines falls within the scope of Community law, but on the other hand, it indicated that the data transfer for public security reasons of the same data does not benefit from the protection of the 1995 Data Protection Directive. In his initial reaction to the PNR judgment, the European Data Protection Supervisor pointed out that this reasoning creates a loophole in the protection of citizens. The judgement seemingly implies that the transmission of information to third countries or organisations from the future Visa Information System or SIS II would not be subject to the applicable rules of the 1995 Data Protection Directive, as long as the transmission is intended for police or public security use.

The practical results of the ECJ decision were, first, that the First PNR Agreement between the EU and the USA needed to be replaced, and, second, that the Second PNR Agreement would need to follow Third Pillar processes. Negotiations for the conclusion of the Second PNR Agreement began on July 2006, and were this time led by the Council. The Council authorised “the Presidency, assisted by the Commission, to open negotiations for an Agreement with the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security”. However, given the tight deadline and tense feelings raised within the EU by the Court’s decision, its conclusion by September 2006 seemed unrealistic, so that an Interim PNR Agreement was suggested that would remain in effect until the end of 31 July 2007, when the second PNR Agreement should be concluded.

77. See Article 35 (3) EU Treaty.
78. In this light, the PNR judgment contrasts with the more liberal approach of the ECJ in its earlier judgment in the Österreichischer Rundfunk case.
79. EDPS first reaction to the Court of Justice Judgment, 31 mei 2006 <www.libertysecurity.org/article985.html>.
In accordance with Third Pillar procedures, negotiations between the USA and the (Finnish) Presidency, “assisted by the Commission”, were completed on October 6, 2006. On October 16, 2006 the Council adopted a decision “authorising the Presidency to sign an Interim Agreement with the United States on the continued use of PNR data”. The Interim PNR Agreement entered into force on October 18, 2006.

The Interim PNR Agreement accepts that “in view of the Undertakings issued on 11 May 2004 by DHS, Bureau of Customs and Border Protection, the United States can be considered as ensuring an adequate level of protection for PNR data transferred from the European Union concerning passenger flights to or from the United States”. Consequently, the Undertakings upon which the First PNR Agreement was based are considered, for the Interim Agreement’s purposes, as being still valid and ensuring an ‘adequate’ level of protection.

The distinction between pillars is a source of complexity, also with regard to data protection. From a legal point of view, the European Court of Justice has been clear in its judgement: the only factor to take into account in order to determine the scope of data processing is the nature of the processing itself, as opposed to the origin of the data. In this sense, the idea that the judgement creates loopholes in EU legislation could be discussed. Indeed, all processing either needs to be included in the exemptions to Directive 95/46/EC, or to fall under the terms of the Directive.

Despite the fact that such legal loopholes may not exist as such, it is undeniable that the “use of commercial data for law enforcement purposes” requires special protection provisions, different from those currently offered under the EU Third Pillar. As a result of the sectoral or piece-meal regulatory approach of data protection in this field, new legislation needs to be introduced with each new technology or new processing operation (supra). Again, this approach is not inherently wrong, although it may not always be desirable for the law to continually have to catch up with developing new practices. The real problem is that, in general, having to regulate data protection within Third Pillar institutions is far from easy and ideal. Member States have a greater say in the Third Pillar structure. So far, few commentators have defended the view that this structure has produced a good balance between security and privacy. This contrasts with the First Pillar, which offers institutional specificities such a reinforced participation of the European Parliament and a stronger role of the European Court of Justice, as well as more consistent data protection.
As we have seen, one of the major differences between EU data protection in the First and Third Pillars is that today there is no formal general requirement in the latter to declare that a third country ensures ‘adequate’ data protection to allow the transfer of data to said country. The second version of the PNR agreement signed between the EU and the US, approved in the framework of the Third Pillar, is nevertheless based on a Council Decision stating that ‘adequate’ protection will be provided by US authorities. The fact that such ‘adequate’ protection might indeed be provided is currently the subject of heated discussion, but it is probably impossible to prove. The general difficulties encountered by the EU in reviewing such ‘adequacy’ for US processing under the First Pillar, are compounded by the specific review limitations related to security matters. If it is not required by EU legislation to formally declare that the US authorities offer ‘adequate’ data, if it is possibly not even accurate and in any case subject to debate, then the point of making such a statement can be questioned.

3. The Swift case

The credibility of the current EU data protection system has also been undermined by the so-called ‘SWIFT case’, which also showed that serious violations of data protection law manage to escape the supervision of the data protection authorities and finally need to be addressed at a different, political level. Swift (‘Society for Worldwide Interbank Financial Telecommunication’) is a worldwide financial messaging service that facilitates international money transfers. Swift stores all messages, including the personal data they contain (such as the names of payers and payees) for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to as ‘mirroring’. After the terrorist attacks of September 2001, the United States Department of the Treasury (UST) issued subpoenas requiring Swift to provide access to message information held in the USA. Swift complied with the subpoenas, although certain limitations to UST access were negotiated. Being a Belgian based cooperative, Swift is subject to Belgian data protection law implementing the 1995 Data Protection Directive. Moreover, the financial institutions in the EU using Swift’s services are subject to national data protection laws implementing the Directive in the Member State in which they are established.

The case became public as a result of press reports in late June and early July 2006, leading to reactions by the Belgian government, the Belgian data protection authority, the EDPS and the Article 29 Working Party. Like most national supervisory authorities, the EDPS conducted an inquiry
within its competence, focusing on the role of the European Central Bank. The Article 29 Working Party called upon Swift and the EU financial institutions to take measures to remedy the illegal current state of affairs without delay. It declared, on 26 September 2006, that it considered it a “priority to safeguard European data protection rights”, that it criticised the lack of transparency surrounding the arrangements with the UST and that it called for clarification on the oversight on Swift. On 22 November, the Article 29 Working Party unanimously adopted an opinion on the access by US authorities to EU banking data through Swift, in which the EU data protection authorities observed that both Swift and its client financial institutions shared joint responsibility, although in different degrees, for the processing of personal data as ‘data controllers’ within the meaning of Article 2(d) of the Directive. Although Swift bears the primary responsibility for the personal data transferred to the US, the financial institutions are also responsible for the way their clients’ personal data are processed. This responsibility is now at stake, according to the Working Party, since continued transfer to the UST is a ‘further purpose’ not compatible with the original commercial purpose for which the personal data have been collected, within the meaning of Article 6(1)(b) of the Directive. The Article 29 Working Party stressed that in the Swift case there had been neither an adequate legal ground for the measures taken, nor independent control by data protection supervisory authorities. The hidden, systematic, massive and long-term transfers of personal data to third country authorities that had taken place, therefore constituted a violation of the fundamental principles of European data protection law.

Moreover, Swift could not rely on Article 25 of the Directive providing that the transfer of data to a third country might take place only if the third country in question ensures an adequate level of protection. None of the exemptions to this principle in Article 26 (1) of the Directive apply to the processing of data in the USA. Swift did not make use of the mechanisms


82. Neither Swift nor the financial institutions in the EU have provided information to data subjects about processing of their personal data, in particular as to the transfer to the USA, as required under Articles 10 and 11 of the Directive. The control measures put in place by Swift, in particular regarding UST access to the data, in no way replace the independent scrutiny that could have been provided by supervisory authorities established under Article 28 of the Directive.
under Article 26(2) of the Directive to obtain authorisation from the Belgian data protection supervisory authority for the processing operations.

It is not clear whether the Swift case will lead to court proceedings or not, as there seems to be little political will to go that far even if some contend that the Commission could take legal action against the Belgian government for failing to ensure Swift compliance with EC regulations. It is clear however that all parties involved (Swift, financial institutions and Central banks) need to act to ensure that international money transfers occur in full compliance with data protection law, and to put an end to the regrettable lack of transparency which characterised the Swift case. The case is interesting because it highlights the legal uncertainty that governs EU data protection, especially after the PNR judgement. On the basis of the judgement, it could be argued that the 1995 Data Protection Directive does not apply, since the transfer serves enforcement purposes. This would imply that all depends on the national – especially Belgian – data protection laws. However, if the Directive does not apply, how could the Commission take legal action against national governments? There is a risk of ‘loopholes’ in the EU system of data protection, and there is most certainly a growing need to close them. Or is the EU again planning to create piece-meal regulation with specific data protection provisions? A question that has not been asked so far been raised is whether the Member States will always accept ad hoc interventions by the EU? What will happen if, in a case like the Swift case, one or more Member States oppose EU intervention and prefer to cooperate with third countries on their own terms (terms that will most likely not be supported by high data protection standards)?

IV. The draft Framework Decision on the protection of personal data in the field of JHA

Although some policy makers still question the need for a general data protection framework for the Third Pillar, pressure by the European Parliament and growing insight into the matter has led to the elaboration

84. We repeat that there are good arguments for this position. The piece-meal regulation that has been produced so far is often of good data protection quality and in the case of Schengen, Europol and Prüm tailor-made in an exemplary manner.
of a new standard text on data protection in the Third Pillar, based on EU legal instruments (not on a Council of Europe Convention) to replace or complement the specific provisions governing initiatives such as Schengen, Europol and Eurojust.

On 4 October 2005, the Commission forwarded a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (“DPFD”) to the Secretary-General of the Council.\(^85\) On 13 December 2005, the Council consulted the Parliament on the proposal. The Parliament delivered its opinion on 27 September 2006. The European Data Protection Supervisor also delivered his opinion\(^86\) on the proposal, which he presented to the Multidisciplinary Group on Organised Crime (MDG)-Mixed Committee on 12 January 2006. On 24 January 2006, the Conference of European Data Protection Authorities also delivered an opinion\(^87\) on the proposal. The Commission presented its proposal to the meeting of the Council's Multidisciplinary Group on Organised Crime (MDG – Mixed Committee) on 9 November 2005. The MDG discussed the proposal at length and completed the third reading at its meeting on 15 and 16 November 2006. The work of the Commission and the interventions of the Multidisciplinary Group on Organised Crime was received with little enthusiasm. Lack of consensus within the group explained why in January 2007 the German Presidency, admitting that the Council had reached a stalemate, asked the European Commission to go back to the drawing board and prepare a ‘revised’ proposal.\(^88\) At the meeting of the Article 36 Committee on 25 and 26 January 2007, the Presidency set out a series of basic guidelines\(^89\) for revising the proposal, with the aim of removing outstanding reservations and making a real improvement in Third-Pillar data protection. The Presidency’s revised draft of 13 March 2007 reflects

\(^86\) 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864.
\(^87\) 6329/06 CRIMORG 28 DROIPEN 12 ENFOPOL 26 DATAPROTECT 4 COMIX 156. 7315/07.
\(^88\) See page 4, point 7 in Presidency Note for discussion at the Article 36 Committee on 25-26 January: EU doc no: 5435/07.
\(^89\) 5435/07 CRIMORG 12 DROIPEN 4 ENFOPOL 5 DATAPROTECT 3 ENFOCUSTOM 9 COMIX 57.
those guidelines.\textsuperscript{90} We first discuss briefly the general structure of the proposed text, and then address the provisions governing transfers of data to third countries.

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 followed at least the pattern of the Directive.\textsuperscript{91} Consequently, both the structure of the proposed Framework Decision and its approach to its subject matter is influenced by the Directive. The headings of the proposed Framework Decision are similar to those of the Directive and they cover scope and definitions in Chapter I, the general data protection principles in Chapter II, individual rights in Chapters IV, V and VI, the establishment of a Supervisory Authority (to be assisted by a Register) and a Working Party in Chapter VII. Only Chapter III of the proposed Framework Decisions, which defines the special types of processing and data transfers (principle of availability), is entirely unprecedented.

Like the Commission Proposal, the Presidency’s revised draft of 13 March 2007 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 countries. Modifications and amendments are suggested within all chapters of the draft; however, the most important and most far-reaching innovation made in this 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 Schengen Information System, Europol, Eurojust, and the Third-Pillar Customs Information System, into

\textsuperscript{90} 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, Brussels, 13 March 2007 (15.03). The draft was submitted to the Article 36 Committee at its meeting on 22 and 23 March 2007. The first reading by the MDG was scheduled for 29 and 30 March 2007.

\textsuperscript{91} See Original Council Proposal, p.4. The Commission indicated 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”.

331
a single data protection supervisory authority, merging with it the advisory working party provided for in the earlier draft.

With regard to transfers of data to third countries, the October 2005 Commission proposal sets up a system similar to that of Directive 95/46, allowing some central control over the third countries to which national law enforcement agencies would send data. The Multidisciplinary Group on Organised Crime was very critical of this part of the proposal, preferring to leave the task of taking ‘adequacy’ decisions to Member States. This position is echoed in the Presidency’s revised draft of 13 March 2007. There is almost nothing in the draft on transfers to third countries. In the Preamble, it is said that where “personal data are transferred from a Member State of the European Union to third countries or international bodies, these data should, in principle, benefit from an adequate level of protection”, but nowhere in the text is there an indication of the procedure or the criteria to be applied when assessing this norm. On the contrary, it is said that bilateral agreements undertaken by Member States are expressly not affected by the Framework Decision, which could ultimately lead to problematic situations where, for instance, Belgium may deem that Nigeria provides ‘adequate’ protection, and thus exports its police records to it, while, at the same time, France thinks otherwise and prohibits such exports. In this example, a major problem could arise if Belgium acquired data from France under the principle of availability and wanted to send the data to Nigeria. For this type of situation, the Multidisciplinary Group on Organised Crime seems to have accepted as a last resort to require 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”.

In the Presidency’s revised draft of 13 March 2007, this consent requirement is incorporated in Article 14 (‘Transfer to competent

93. Recital 12.
94. The final provisions (Chapter VII) now regulate the relationship to agreements with third countries saying that “This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States or upon the European Union by virtue of bilateral and/or multilateral agreements with third States” (Article 27).
95. See Art. 15(c) of Council’s document 13246/13.11.2006 (available at: http://www.statewatch.org/eu-dp.htm).
International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift

authorities in third States or to international bodies). Altogether, the model is weak and cannot be compared to the stronger central control of the First Pillar, and this even though the need for data protection is even more obvious in the Third Pillar than it is in the First Pillar.

V. Summary and Conclusion

The objective of this contribution was to assess the European Union's regulatory framework for data protection, in particular by comparing the approach under the First and Third Pillars. The starting point of the analysis was the fact that under the First Pillar, which covers all commercial processing of personal information, Directive 95/46/EC provides a common denominator for data protection, but that under the Third Pillar, which covers all crime-related and security-related processing of personal information, such a common standard does not exist at present, but that instead, a patchwork of data protection regulations covers different sector-specific processing (including the Schengen Agreement, SIS II, Europol, Eurojust and, recently, the Prüm Treaty).

In this contribution we have assessed the regulatory framework in the EU with regard to data protection, by contrasting the comprehensive model of regulation, as used for the First Pillar, with a sectoral or piece-meal approach, as is presently being used for the Third Pillar (section II). Section II A briefly highlighted the main features of the data protection system established by Directive 95/46/EC and Regulation 45/2001. It also briefly analysed the indirect impact of the First Pillar system on Third Pillar data transfers.

In sections III we discussed whether a European approach would be required to data transfers to third countries. Whereas such a European approach, based on the adequacy principle, is followed in the First Pillar, this is not the case for the Third Pillar. Though there may be arguments against such a European approach in the area of JHA (section III C), we analysed several cases, including the Europol, PNR and Swift cases, in which the absence of such a European approach was believed to have caused problems (section III D).

96. “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”.

333
Without ignoring the benefits and arguments in favour of tailor-made regulations, we came to the conclusions that the example of Europol dealing with third countries, and of PNR and Swift, in part illustrated the lack of credibility of the current EU data protection system. Having to deal with externalities such as powerful third countries (in particular the U.S.) that do not always consult the EU officials when collecting 'European' data or data in (some) EU Member States, it would in our belief be beneficial to develop a general framework for data protection in the Third Pillar and for transfers of data to Third Parties with clear rules and responsibilities and a well-defined role for the EU institutions that live up to the European dimension behind cases such as PNR and Swift. We would even agree with Poullet that a uniform set of data protection standards applicable to all pillars would be desirable.

In this respect the 2005 Commission proposal for Council Framework Decision on data transfers to third countries was a welcome step forward. However, the scarcity of the provisions on transfers of data to third countries in the revised draft proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters of 13 March 2007 is not to be applauded and contrasts with the October 2005 Commission proposal setting up a Directive-like system, allowing some central control on the third countries to which national law enforcement agencies would send data. There might be good reasons for the Multidisciplinary Group on Organised Crime preferring to leave the task of taking 'adequacy' decisions to Member States. As a matter of fact there might be reasons to transfer data in the field of JHA even when there is no adequacy in a Third State, but these reasons do not justify the complete repudiation of a Directive-like system and its replacement by the current proposals. One can hope that the current choice for a system that relies on Member States will trigger a learning process between Member States leading, in the long-term, to the 'best' solutions becoming the rule.

In more general terms we have come to the conclusion that processing of personal data in the field of JHA is in need of a general framework with harmonized rules that avoid the risk of harmful regulatory competition between the regulatory regimes of the EU Member States, and that contribute to effective privacy protection by avoiding distortions resulting from the externalities which a purely decentralized model of implementation of data protection would risk ignoring. 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 in October 2005. The proposal did meet with strong resistance by the Member States, but it is our conviction that their alternatives are less satisfactory on the issue of regulating transfers of data to third countries. A net result of the latest proposal would be that the EU would be obliged to invent data protection standards on the issue, over and over again, with every new issue or demand to cooperate with third countries. This is clearly not an example of good regulation.
