Towards a coherent EU policy on outgoing data transfers for use in criminal matters?

The adequacy requirement and the framework decision on data protection in criminal matters

A transatlantic exercise in adequacy

Els De Busser
Gert Vermeulen

1 The need for coherency

Personal data or data that enable the identification of a natural person are due to their inherent link to the right to a private life, protected by a specific set of rules within the European Union (further: EU). These rules provide protection on the level of collecting these data and subsequently using them.

The origin of the EU's data protection rules really lies in the first pillar where the creation of an internal market in the EC ensured the free movement of goods, persons, services and capital between the member states. Removing all obstacles to realize this free movement includes removing restrictions on trade. As restrictions are often the result of divergent national legislations, a certain level of approximation was considered necessary for the functioning of the common market. Including also the flow of personal data in the free movement of goods and services (De Hert, 2004, p. 7), harmonised rules were needed on the level of personal data protection. In order to protect these harmonised data protection systems, the same values should be sustained when transferring personal data outside the internal market and to third states or institutions.

Although the Council of Europe (further: CoE) took the lead in drawing up the standards, the consensus within the EU to copy and implement them, was in first instance broad. With the right to a private life protected by the European Convention for the protection of human rights and fundamental freedoms (further: ECHR), which allows room for derogating from it, a similar approach was taken to the data quality standards.

With its wide scope of automatic processing of all personal data, the CoE's Convention for the protection of individuals with regard to automatic processing of personal data (ETS N° 108, 18 January 1981; further: data protection convention) served as a basis for copying the same standards in more specific instruments.

While data processing in the course of activities falling within the scope of Community law was governed by a set of binding instruments (Directive 95/46/EC,

O.J.L, 23 November 1995, issue 281, p. 31-50) Directive 2002/58/EC on data processing in the telecommunication sector, *O.J.L*, 31 July 2002, issue 201, p. 37-47) and Regulation 45/2001 on data exchange between Community institutions or bodies or to third institutions or bodies, *O.J.L*, 12 January 2001, issue 8, p. 1-22), data processing by judicial and law enforcement authorities within the third pillar had to rely on national law or on the general data protection convention.

As part of an area of freedom, the need for an instrument on data protection in the third pillar was felt and expressed in the 1998 Vienna Action Plan and planned to be developed by 2000 (*O.J.C* 23 January 1999, issue 19, § 7 and § 47). Despite numerous efforts (see inter alia Council, 6316/2/01, 12 April 2001; Commission, COM(2005) 475 final, 4 October 2005 and Council, 7315/1/07, 24 April 2007), the Council has been working for more than five years on a proposal for a Framework Decision member states can agree on. Creating a coherent data protection instrument in the third pillar proved to be a challenge, not in the least because of the involvement of the member states in the decision making process (see also De Hert and De Schutter, 2008, p. 329-333).

The Council agreed on framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (further: framework decision on data protection in criminal matters) of 24 June 2008, which was formally adopted in December 2008 (*O.J.L* 30 December 2008, issue 350, p. 60-71). The instrument entered into force in January 2009.

The expectations were high as this new instrument was supposed to answer to the need for a coherent policy that is custom-made for the exchange of personal data in criminal matters. The need for coherency was particularly high when the transfers of personal data to third states or institutions was concerned. Protecting personal data that are processed within the borders of the EU includes protection for exchanging these data with third states or institutions as the recipients are not necessarily bound by the same data protection principles. The solution was found in requiring the receiving state or institution to provide in a level of data protection that was adequate in comparison to the EU standards so personal data could safely cross the external EU borders. However, legal instruments covering data protection do not provide in rules on this type of protection or are not generally binding throughout the EU. (see also De Hert and De Schutter, 2008, p. 309)

The need for a coherent policy on data transfers to third states or bodies was nevertheless not fully answered by the new framework decision. Its partial scope, the possible derogations to the requirement of adequacy, the lack of a uniform assessment and the effects of the new instrument on existing and future provisions, make the framework decision an inappropriate instrument for mending the inconsistencies in the third pillar's data protection policy towards outgoing data transfers.

In agreements that have been concluded between the United States of America (US) on the one hand and the EU (Agreement 25 June 2003 on mutual legal assistance between the European Union and the United States of America, *O.J.L.* 19 July 2003, issue 181, p. 34-42), Europol (Agreement between the United States of America and the European Police Office, 6 December 2001) and Eurojust (Agreement between Eurojust and the United States of America, 6 November 2006) on the other hand, the adequacy requirement is losing its significance by a lack of application or by being

excluded from the agreement altogether. This is however not the case in every agreement with a third state.

The last and most recent negative effect on the adequacy requirement is visible in the preparatory future plans for the EU's justice and home affairs policy for 2010-2014 (The Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), Report, Freedom, Security, Privacy – European Home Affairs in an Open World, June 2008 and High-Level Advisory Group on the Future of European Justice Policy, Proposed Solutions for the Future EU Justice Programme, June 2008). These functioned as the *travaux préparatoires* for the so called Stockholm Programme (COM (2009) 262/4), the successor of the Hague Programme. Again with regard to the transatlantic cooperation in criminal matters the adequacy of the level of data protection in the US is assumed rather than thoroughly examined.

In this contribution the EU's policy on data exchange in criminal matters to third states or institutions is first studied from the perspective before and after the framework decision on data protection in criminal matters. Secondly, the provisions of the framework decision that regulate the outgoing data transfer – including the effects on existing and future provisions – are examined. In a third and final part, the future of the adequacy requirement in agreements with third states and as included in the policy plans of the EU is reflected on.

2 Before the framework decision

Before the framework decision on data protection in criminal matters was developed, binding provisions on data protection were limited to the CoE instrument applicable to all automatic personal data processing or the EU's first pillar instruments. The requirement to ensure an adequate level of data protection in the receiving state or institution is intended to protect the EU standards on data protection whenever personal data are exchanged with a national authority or an institution located outside the EU territory. With regard to data transfers to third states or institutions, this requirement has first been included in Directive 95/46/EC regarding data transfers for the purpose of activities within the scope of Community law. In 2001 the requirement was included in the 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 (ETS, N° 181, 8 November 2001; further: the additional protocol to the data protection convention). Also specific data protection provisions in the relevant Eurojust and Europol instruments, provide in the requirement.

However, a general rule on ensuring an adequate level of data protection in the receiving state or institution was inexistent for the field of criminal matters.

2.1 Limited rules on data transfers to third states or institutions

The instruments that provide in rules on data transfers to third states are limited. The Council of Europe's data protection convention encompasses basic rules for data protection in view of a trans-border exchange to a contracting party. All EU member states have ratified this convention. Thus, the exchange of personal data between mem-

ber states – with a view to the automatic processing of data – should run in accordance with the data quality standards provided by the data protection convention.

However, no rules are provided when sending data directly to a state that has not ratified the convention and is therefore not necessarily bound by the same principles. Only the indirect transfer of personal data is regulated as the convention foresees the situation in which a state party transfers personal data to a third state via the territory of a state party. In that case, exceptionally, the transferring state is allowed to lay down additional protective rules (prohibitions or added requirements of authorisation) if these serve the purpose of maintaining the level of data protection and avoiding the circumvention of the legislation of the transferring state.

Directly sending personal data from a state bound by the data protection convention to a state that is not party to the convention is regulated by the 2001 additional protocol. The instrument provides in an additional requirement that encompasses an examination of the receiving state's data protection system. The system needs to be assessed on its adequacy in relation to the standards laid down by the data protection convention. However, it was not the additional protocol that introduced the adequacy requirement.

For activities within the scope of Community law, Directive 95/46/EC subjects the outgoing data transfers to the requirement of adequacy. No personal data can be sent to a state that does not pass the assessment of its legal framework on data protection. The prerequisite ruffled a few feathers in third states' authorities (Boehmer and Palmer, 1993, p. 307-308; Bennet and Raab, 1997, p. 245-263 and Long and Quek, 2002, p. 334-337). In the cooperation with the EC, the entry into force of Directive 95/46 caused the US to take action in ensuring the protection of data received from the EC. The processing of data that is aimed at here is the processing for the purpose of trade with US companies. Data protection by US companies does not fall within the scope of a general legislation but is regulated by sector specific rules and self-regulation (Banisar and Davies, 1999, p. 13-14; Long and Quek, 2002, p. 330 and Levin and Nicholson, 2005, p. 362. See also C.A. Ciocchetti, 2008, p. 1-45). In order to make this system adequate, additional guarantees were needed in the shape of the so-called Safe Harbour compromise funded on the principles of notice, choice, onward transfer, security, data integrity, access and enforcement (Safe Harbour Privacy Principles issued by the US Department of Commerce, 21 July 2000). The compromise largely consists of a choice for private companies to either enter into a self-regulatory privacy program that meets the terms of these seven principles, either design their own self-regulatory privacy procedure on the condition that the Safe Harbour principles are complied with (Long and Quek, 2002, p. 325-344).

2.2 The adequacy requirement: not generally binding and diverse implementation

The provisions on requiring an adequate level of data protection in the third state concerned, are aimed at protecting the recognized standards outside the external borders of Europe. Assessing the standards utilized in the receiving state or authority can ensure an appropriate level of data protection after the exchange. This means that the basic principles for data protection valid in the EU are scrutinized as to the extent they are complied with in the receiving state or authority. Two points of view should be taken into consideration here, firstly the case in which an EU member state

authority wishes to send personal data to a third state or authority and secondly the case in which the EU bodies Europol or Eurojust want to make such transfer. In both cases, the assessment can be made on a case-by-case basis or for an entire state or institution.

2.2.1 Member states

When EU member states' authorities receive a request from a third state or authority for personal data to be transferred, the adequacy requirement is applicable when the requested state has ratified the additional protocol to the data protection convention. This protocol specifies the necessity of an assessment of the level of data protection to be offered by the receiving third state or authority. However, this provision does not include detailed rules on how to carry out the assessment.

Nonetheless, it is clear that in order to maintain data quality standards when giving personal data into the hands of an authority that is not bound by the same standards, the criterion of adequacy functions as the umbrella concept of an appropriate level of data protection. The basic principles encompassed by the data protection convention – more specifically in Chapter II of the convention – must be taken into account while assessing the adequacy of the third states' legal framework on data processing. Unfortunately, the explanatory report states that this clarification is only valid as far as these principles are relevant for the specific case of transfer (ETS no. 181, 8 November 2001, Explanatory report, §29).

This allows for differences in evaluation tools and methods as well as items – such as the data quality standards – included in the evaluation, to result in divergent outcomes depending on the state carrying out the assessment. From the point of view of the third state that requests personal data from two states that have ratified the additional protocol, this can lead to a different reply from each state (European Data Protection Supervisor (further: EDPS), *O.J.C* 26 April 2007, issue 91, p. 12 and EDPS, *O.J.C*, 23 June 2007, issue 139, p. 6). Hence, as long as no uniform checklist of the minimum provisions covered by an adequate level of data protection is available, this could lead to *data-shopping*.

To allow for some flexibility on the part of the exchanging states, the additional protocol provides in derogations from the adequacy requirement, that should be interpreted restrictively. National law must first of all provide in the transfer. Additionally, the transfer of personal data is only permitted when legitimate interests – especially important public interests – prevail over the lack of an adequate level of data protection. Not coincidentally, the explanatory report refers to the same interests based on which the right to privacy and the data quality principles can be lawfully derogated from (ETS no. 181, 8 November 2001, Explanatory report, §31).

Apart from the allowed derogations, in case an adequate level of data protection cannot be assured another possibility for exchange exists if the receiving state provides in sufficient safeguards such as the Safe Harbour compromise. The latter could nevertheless seem to amount to requiring adequacy. However, the safeguards could be limited to only the relevant elements of data protection (ETS no. 181, 8 November 2001, Explanatory report, §32-33). This means that the safeguards should be customized to the case – i.e. the tie between requested and requesting party which could be a contract

or an agreement between states or institutions – and do not have to encompass all principles included in the EU standards on data protection.

Nevertheless, so far only sixteen member states have ratified and are thus bound by the protocol. EU member states are only bound to comply with the adequacy requirement in criminal matters when they belong to this group of sixteen states or when they have provided this rule in their national legislation on data protection in criminal matters. The few member states that have – on their own initiative – widened the scope of their legislation implementing Directive 95/46/EC to include criminal matters, will also be bound by the adequacy requirement. Nonetheless, the requirement of checking the adequacy of the receiving data protection system is thus not a generally binding requirement in the EU.

2.2.2 Eurojust and Europol

The EU institutions involved in data exchange with the national judicial and law enforcement authorities, Eurojust respectively Europol, have developed their own data protection regulations. Equally here, the picture is diverse.

The Decision setting up Eurojust provides in the adequacy requirement for the data transfers to a third state or body (Council, *O.J.L* 6 June 2002, issue 63, p. 1-13). Without an assessment of this third state or third body's data protection system, Eurojust is not allowed to transfer personal data. Referring to the data protection convention, the assessment of the level of protection shall be made in the light of all the circumstances for each transfer or category of transfers. In order to make a complete evaluation, all elements of the transfer should be included, i.e. the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the state or organisation in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer. The assessment is made by Eurojust's data protection officer and only involves the Joint Supervisory Body (further: JSB) when difficulties are met during the process. The amended decision on strengthening Eurojust does not add to these provisions in order to improve the assessment (Council, 5347/09, 20 January 2009), even though the European Data Protection Supervisor has called upon the Council to use this opportunity to introduce the approval of the JSB in the procedure (European Data Protection Supervisor, 9013/08, 7 May 2008, §36).

In comparison with Europol, however, the set of rules governing the adequacy check for Eurojust's third state transfers is not particularly detailed (Council, *O.J.C* 30 March 1999, issue 88, p. 1-3.

With the exception of urgent circumstances, a four-step filter needs to be passed to conclude an agreement with a third state or body. This filter starts with a report by the Management Board stating that no obstacles exist to start negotiations. The JSB needs to be consulted on this subject as well. During this stage, a first check of the third state or body's data protection system can already be made as the JSB protects the rights of the individual regarding the processing of data by Europol.

Subsequently, a unanimous decision by the Council is needed (Council, *O.J.C* 13 April 2000, issue 106, p. 1-2). During this stage, a second check of the third state's data protection is made as the Council should consider the law and the administrative

practice of the third state or body in the field of data protection, including the authority responsible for data protection matters.

In a third step, the Director will start negotiations, after which the Management Board and the JSB will need to give their approval to conclude the agreement in a final step (De Hert and De Schutter, 2008, p. 319-320).

The only cases in which this four-step approach is not followed, are the exceptional cases in which Europol's Director considers the transfer of the data absolutely necessary to safeguard the essential interests of the member states concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime. The adequacy evaluation should be done by the Director and supervision is then limited to a post-transfer check and only on request of the Management Board and the JSB.

This implies the responsibility of the Director to evaluate the level of data protection supported by the third state or body before making his decision, instead of the lengthy four-step process. An explicit requirement to verify the adequacy of the receiving state or body's data protection system is not included.

Providing in an option of a post-transfer check of adequacy as opposed to a prior evaluation by several bodies, means that in cases where the level of data protection would be considered not to be adequate, this could only affect possible future transfers to that same third state or body instead of blocking a currently planned transfer.

When the recently adopted Europol Decision (Council, 8478/09, 6 April 2009) enters into force, the four-layered adequacy check remains intact as a general rule for transfers to third states or bodies.

In exceptional cases however, the aforementioned implied adequacy check is given a new meaning. The obligation for the Director to consider the data-protection system of the receiving body in question should be carried out with a view to balance the data-protection level and the interests protected by the transfer. This means that the adequacy requirement does not need to be fulfilled, a fortiori is derogated from in an unspecified manner (EDPS, *O.J.C* 27 October 2007, issue 255, § 29).

2.2.3 Inconsistent requirement

Even with the sensitivity that is inherent to the field of criminal matters, the requirement of adequacy is not laid down for every transfer of personal data that can be made for purposes of prevention, detection, investigation and prosecution. In addition to the lack of a standard requirement for outbound data transfer, the adequacy rule is not uniformly employed either. The latter is visible on two levels. Firstly, a checklist of data protection rules that should minimally be evaluated while making the adequacy assessment is not provided by the EU. Secondly, while Europol has developed a multi-level adequacy assessment, Eurojust relies on its data protection officer. This means in practice that an individual can see his or her personal data transferred from a member state to a third state and being used in that particular third state for incompatible purposes. For example, an individual's personal data on receiving a weapon permit in a member state could be transferred to the third state and used against this person in a custody case. Additionally, due to the lack of uniform assessment systems, this example could be reality when dealing with one third state but not with the other. Obviously, this opens the door to unjustified discriminating between identical cases.

The new framework decision on data protection in criminal matters could have ensured more coherency in the EU's third pillar by answering to these concerns.

3 Inadequacy based on purpose deviation

One of the elements in need of particular consideration when assessing the adequate level of data protection is the compliance with the purpose limitation principle (article 13, §4 of the framework decision on data protection in criminal matters). The principle restricting the use of personal data to the purpose they were gathered for or a compatible purpose should also be complied with by the receiving state or authority. Given the – often significant – differences between the structure of states' criminal justice systems and the competences of their respective authorities, living up to the purpose limitation rule is particularly important when transferring personal data to a third state. In view of the EU's cooperation in criminal matters with the United States (further: the US) and the agreements concluded between the EU, Europol and Eurojust on the one hand and the US on the other hand, the adequacy of the American data protection level should have been tested, including the purpose limitation rule.

3.1 Purpose limitation to purpose deviation

Personal data should be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. Thus, personal data should only be processed for purposes identical to the purpose they were gathered for or a compatible purpose. This principle of purpose limitation has been laid down in the data protection convention and was copied into Directive 95/46 for activities of Community law. Purpose limitation incorporates an aspect of foreseeability by the data subject who should be in a position to anticipate in which cases his or her personal data can be gathered and in which cases these data can be processed and by whom (European Court of Human Rights (further: ECtHR), *Leander v. Sweden*, 1987, § 48 and ECtHR, *Rotaru v. Romania*, 2000, § 46 and European Data Protection Supervisor (further: EDPS), *O.J.C*, 23 June 2007, issue 139, § 20; see also Bygrave, 2002, p. 337-341). In other words, personal data gathered for the purpose of commercial activities should not be used for purposes incompatible with commercial activities, such as prevention, detection, investigation and prosecution of criminal offences. If that is the case, the data subject did not have the opportunity to react – read: object – against the final purpose for which the data are processed. Still, in cases that this is necessary for a legitimate goal and laid down by law, the deviation from the original purpose is allowed.

The purpose limitation principle thus leaves room for the use of personal data for other purposes than the initial purpose, as long as there is compatibility between the two or as long as the conditions for allowed derogations are fulfilled. Nevertheless, this possibility is stretched to a point where there is no compatibility between the original purpose of gathering and the final purpose of processing the data (De Busser, 2009a, p. 163-193). This development to purpose deviation rather than purpose limitation seen in the EU's instruments on data exchange between the law enforcement and judicial authorities of the member states as well as data exchange within the EU involving Europol and Eurojust.

In several legal instruments, personal data gathered for EC-related purposes are used in criminal matters. In administrative investigations conducted by the EC's anti-fraud unit OLAF, personal data that are discovered should be secured and the case left to the competent judicial authorities. The OLAF decision thus provides a formalized purpose deviation from the OLAF investigation to national authorities (European Parliament and Council, *O.J.L* 31 May 1999, issue 136, p. 1-7). Even between Eurojust and OLAF an agreement on the transfer of personal data has been signed (Practical Agreement on arrangements of cooperation between Eurojust and OLAF, 24 September 2008). For both types of transfer of personal data from OLAF no lawful derogation to the purpose limitation rule can be called upon to justify the transfer between the first and third pillar.

Other paths have been opened for Eurojust as well as Europol to gain access to personal data that have not been gathered for the purpose of criminal matters. New developments in the Schengen Information System (further: SIS) – the so-called SIS II that should be operational by the end of 2009 – create opportunities for Eurojust, Europol and for law enforcement authorities to access the database that was originally designed for border management purposes (Council, 14914/06, 12 December 2006). Initially intended to broaden the capacity of the existing SIS in order to pave the way for new member states to join, the momentum was used to introduce new functions to the system including these new access rights (Council, *O.J.L* 7 August 2007, issue 205, p. 63-84). The requirements for a lawful derogation from the purpose limitation rule are however fulfilled.

In the same spirit, the Commission experienced the lack of law enforcement access to Visa Information System (further: VIS) as a shortcoming and a serious gap in the identification of suspected perpetrators of a serious crime (Commission, COM(2005) 597 final, 24 November 2005, p. 6). This was realized in the 2008 decision granting designated authorities and Europol access to the VIS even though it was designed to establish a common identification system for visa data in the context of a common visa policy for the member states, thus not for any purpose related to criminal matters (Council, Decision, *O.J.L* 13 August 2008, issue 218, p. 129-136). Additionally, due to the delineating of the authorities by means of a functional criterion, equally intelligence services could legally have access to VIS (EDPS, *O.J.C* 25 April 2006, issue 97, p. 9). The necessity requirement should thus be strictly complied with in order to fulfill the conditions of a lawful derogation to the purpose limitation rule.

Granting access to law enforcement authorities to the Eurodac database that was developed as a fingerprint database for asylum purposes, touches upon a similar issue (Council, 11004/07, 19 June 2007 and Council, 11004/07 COR 1, 2 July 2007; Standing Committee of Experts on International Immigration, Refugee and Criminal law, CM0712-IV, 18 September 2007).

Finally, the data retention directive of 2006 obliges telecommunication providers to save certain types of personal data for the purposes of investigation, detection and prosecution of serious crime (European Parliament and Council, *O.J.L* 13 April 2006, issue 105, p. 54-63). This equally means a transfer from the first to the third pillar demonstrating purpose deviation rather than purpose limitation.

It is thus a well-established development in the law enforcement and judicial cooperation in criminal matters between the EU member states, to move into the direction of purpose deviation. Even though purpose limitation is one of the basic principles of

data protection and should thus unquestionably be part of an adequate level of data protection in a third state, it is in the same way left when we look at the EU's cooperation in criminal matters with the United States.

3.2 Adequacy of the American level of data protection

Concluding on the adequacy level of the US data protection system from an EU point of view is challenging due to the different structure of the American data protection system as opposed to the EU's legal framework on data protection (see elaborately De Busser, 2009b, p. 282-291). Where the EU's data protection standards are based on an umbrella instrument – the CoE's data protection convention – that has been ratified by all member states, the US relies on a combination of sector specific legislation, self-regulation by companies and technologies of privacy (Banisar and Davies, 1999, p. 13-14 and Long and Quek, 2002, p. 330). Not only are data protection laws differently structured, also privacy policies in the EU and the US have slightly divergent political and social foundations (Whitman, 2004, p. 1151-1252). Even though the theories concerning these different mindsets could explain and illustrate the situation of data protection in transatlantic relations today and are therefore relevant, they are not the focal point of this contribution.

With regard to the quality of personal data as such, the US starts from the principle of accuracy, relevance and adequacy of personal data. However, the many exceptions to the rule and exemptions made from it, take away the quality of the data. For example, the US Privacy Act explicitly allows law enforcement and intelligence agencies to be exempted from the accuracy check of personal data, unless the data are disclosed to another person than an agency and the data are not asked by means of an request based on the Freedom of Information Act (5 USC §552a; 5 USC §552 and Department of Justice, Overview of the Privacy Act of 1974, 2004 edition, www.usdoj.gov/oip/04_7_1.html). Thus, for an interagency transfer of data, the accuracy standard can be disregarded. Furthermore, the necessity of these exceptions is not motivated and the conditions for lawful derogations are not met.

With regard to the quality of the processing of personal data, the purpose limitation principle does not appear in the US data protection legislation as a general binding rule. This is not problematic as such since many separate provisions apply. However, similar to the EU legal instruments on cooperation in criminal matters, many examples of purpose deviation can be found. Yet, the US deviates from the purpose limitation principle in a different way than the EU. Where the EU opens the use of data after they have been gathered, the US lowers the standards at the moment of data collection.

Firstly, data can be gathered for intelligence purposes and subsequently used for law enforcement purposes. This way, evidence can be introduced in criminal proceedings when it was in fact gathered by using the lower standard of intelligence investigations. The use of administrative subpoenas and national security letters are examples of this technique. For administrative subpoenas, only the possibility of judicial review and a reasonability standard are required (C. Doyle, 2006, p. 2-3). For national security letters, judicial review is not even provided. As long as there is reason to believe that the person or entity on whom information is sought was or may have been a foreign

power or an agent thereof (Department of Justice, Office of Legal Policy, 13 May 2002, p. 7 and C. Doyle, 2008, p. 1-5).

Secondly, investigative techniques that were originally meant for criminal investigations opened for intelligence investigations. This method equally means the use of a technique that, due to its privacy violating character, should be subject to the constitutional requirements of the Fourth Amendment. Nevertheless, the standard is reduced and the data can eventually be used in criminal proceedings. A physical search of private premises should be conducted by applying the Fourth Amendment's rules, however this is brought under the scope of Foreign Intelligence Surveillance Act (further: FISA) (50 USC § 1801 et seq.). The same is valid for the collecting of business records and other tangible objects, by means of the so-called Patriot Act amending FISA (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot Act), Public Law no. 107-56, October 26 2001).

Additionally, the US has a well-established tradition of sharing data among agencies and authorities. An example of this information sharing environment can be found in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law no. 108-458, 17 December 2004) and in the notorious FISA. The latter opened up the wall between the intelligence community and law enforcement authorities by providing in the use of the results from warrantless electronic surveillances for the purpose of criminal proceedings (See also Vervaele, 2005).

With just a few examples shortly assessed from an EU point of view but based on earlier research (De Busser, 2009b, p. 282-291), we demonstrate the lack of an adequate level of data protection in the American system of personal data processing for the purposes of the detection, investigation and prosecution of criminal offences. It is therefore remarkable to see that the EU, Europol as well as Eurojust have rubber stamped this requirement of adequacy instead of making a comprehensive and thorough examination.

3.3 Transatlantic purpose deviation

The EU, Europol and Eurojust have concluded agreements with the US covering the exchange of personal data in criminal matters. The heightened attention for international cooperation in criminal matters after 9/11 had profound consequences on the EU-US relations in the shape of these new instruments. One would thus expect that the adequacy requirement should be complied with and that an assessment of the level of data protection in the US should be available for these agreements. However, this is not the case. On the contrary, the adequacy requirement was negotiated off the table in all three instruments.

The first outcome of the need for data exchange in the transatlantic connection, were the 2001 and 2002 Europol – US agreements. Without any conclusion on the adequacy of the US data protection system, Europol started negotiations assuming that the US was an adequate partner regarding personal data protection. The Europol Joint Supervisory Body (further: JSB) even stated that Europol was unable to express an opinion on the adequacy of the US data protection regime (Europol JSB, 26 November 2001, p. 2). Still, agreements between Europol and other third states – Australia,

Canada, Croatia, Iceland, Norway and Switzerland – include an adequacy assessment. This was therefore not done for the US.

On the contrary, the 2002 Europol-US agreement included a provision that received an interpretation was not seen before in instruments on cooperation in criminal matters. The provisions stating that a 'party to which a request for assistance under the agreement shall endeavor to limit the circumstances in which it refuses or postpones assistance to the greatest extent possible' should – in accordance with the explanatory note – be interpreted as a prohibition on 'generic restrictions' (Council, 13696/1/02, 28 November 2002). The adequacy requirement as one of the basic requirements of the EU data protection framework, more specifically the transfer to third states, is hereby negotiated out of the scope of this agreement.

In addition, the 2002 agreement concerned the exchange of personal data between Europol and the US and included a purpose limitation provision that was much wider than what the EU was used to (Supplemental Agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, 20 December 2002). Especially the interpretation given to the provision in the exchange of notes – including immigration and confiscation proceedings – substantially widened the possible use that could be made of exchanged data (Council, 13996/02, 11 November 2002).

In the 2006 Eurojust-US Agreement (Agreement between Eurojust and the United States of America, 6 November 2006) similar developments are seen with regard to the purpose limitation principle as well as with regard to the adequacy requirement. Since Eurojust has cooperation agreements with states that have ratified the data protection convention – Iceland, Romania, Norway and Croatia – the adequacy requirement was not necessary to fulfill here. However, this was not the case for the US. The cooperation agreement between Eurojust and the US needed to be complemented with a decision on the adequacy of the American data protection level. Yet, no adequacy assessment was made which seemed to not even make the Eurojust JSB bat an eyelid (Joint Supervisory Body of Eurojust, Activity Report 2006, p. 7).

A similar widely formulated purpose limitation rule was applied in the EU-US mutual legal assistance agreement of 2003. Based on articles 24 and 38 TEU, this was done for the first time as a group of member states rather than as separate states (*O.J.L* 19 July 2003, issue 181, p. 34-42). This agreement should – together with the bilateral written instruments developed by the member states – enter into force in 2009.

The adequacy requirement did not make it into the text of the agreement. One could state that the additional protocol to the data protection convention did not enter into force before 2004 and there were no other binding instruments applicable to the EU member states at the time that prescribed this condition for exchanging personal data in criminal matters. However, the adequacy requirement was already included in the additional protocol that was opened for signature in 2001. Thus, the negotiating parties could have anticipated to it and could have included it in the discussions on the content of the mutual legal assistance agreement. Additionally, the requirement was well known from data exchanges outside the field of criminal matters, such as the aforementioned Safe harbour Principles following the Directive 95/46/EC. In spite of many assessments on data protection systems of other third states, the US seems to continuously escape this additional safeguard by acquiring the assumption that its data protection is satisfactory by EU standards.

The purpose limitation rule was equally in this agreement widened to include other purposes. Not included in any of the existing bilateral mutual legal assistance treaties (further: MLATs) between EU member states and the US, the wider rule will replace the existing use limitation provisions in these agreements and will be introduced in the relations with member states that did not have an MLAT with the US yet. The speciality rule that was a traditional part of the MLATs and protected the states' interests is pushed aside (Vermeulen, 2004, p. 103). However, the data subject's interests cannot be considered to enjoy a high level of data protection either due to width of the new rule. In accordance with the new rule, data can be used for unspecified purposes if the requested state – not the data subject – gives its consent. The necessity of this exception to the purpose limitation rule is not clarified.

Purposes for which data can be used are equally widened in specific agreements that have been concluded in order to make the transfer of data between US authorities and EU companies possible. Data gathered for commercial purposes in the EU and transferred and used by US administrative authorities in the fight against terrorism and the financing of terrorism, was the issue in both the case on the transfer of passenger name record (further: PNR) data and the SWIFT case (see also De Busser, 2009a, p. 187-191). In both cases, the relevant US authorities agreed to make commitments regarding the protection of the received data. However, the sharing of data with authorities is a possibility with regard to PNR data (Council, 13738/06, 11 October 2006 and Council, *O.J.L* 4 August 2007, issue 204). The EU agreed to the undertakings by the US on sharing the received data with authorities competent for public security related cases, without a clear necessity indication. In the SWIFT case, the EU also agreed to allow for the data transfer to the US Treasury under the condition of a specific purpose limitation that keeps the use of the data within the limits of terrorist financing investigations and prosecutions. However, it is still an administrative authority receiving commercially gathered personal data for the purpose of criminal investigations and prosecutions.

Purpose limitation is thus not a principle that is equally valued in the EU and in the US. The High Level Contact Group (further: HLCG), a group of senior officials from both sides established to enhance the transatlantic data exchange for law enforcement purposes, attempted to lay down common definitions on key principles (Council, 9831/08, 28 May 2008). The HLCG agreed on the principle that personal data should be processed for specific legitimate law enforcement purposes, in accordance with the law and subsequently processed only insofar as this is not incompatible with the law enforcement purpose of the original collection of the personal information. However, the group overlooked the fact that the term 'law enforcement' encompasses a different landscape of authorities in the EU than it does in the US. The US interprets law enforcement to include border enforcement, public security and national security purposes as well as for non-criminal judicial or administrative proceedings related directly to such offences or violations (EDPS, 11 November 2008, p. 13 and 9831/08, 28 May 2008, p. 4). The title 'common principle' is therefore quite inappropriate.

3.4 Inadequate transatlantic cooperation in criminal matters

Similar to the evolution visible in the EU Legal instruments providing in judicial or law enforcement data exchange, the EU-US cooperation in criminal matters moves

into a clear direction of purpose deviation rather than purpose limitation. Still, it is remarkable that this cooperation was established in the first place due to the lack of an examination of the American level of data protection.

The adequacy requirement was not complied with in the three agreements that have been concluded between Europol, Eurojust and the EU on the one hand and the US on the other hand. *A fortiori*, the prerequisite that should safeguard our data protection standards in criminal justice systems that are not bound by the data protection convention, is eliminated from these agreements in favour of what is called a smoother exchange of data. Even where the requirement is lived up to in the relations with other third states, the US receives the 'approved' rubber stamp without passing the test of providing in adequate data protection.

There is thus no coherency in the application of the adequacy requirement. On the contrary, demanding an adequate level of data protection seems to function as an obstacle rather than as a mechanism of protection, at least in the transatlantic relations in criminal matters. This means that the safeguarding of the European standards on data protection is not appropriately protected in outbound data exchange.

4 The significance of the adequacy requirement in the framework decision

The new framework decision on data protection in criminal matters includes provisions on data processing within the external borders of the EU and provisions on transfers of personal data crossing these borders (*O.J.L* 30 December 2008, issue 350, p. 60-71).

Four conditions are provided in the framework decision for allowing a transfer to a third state of body. Firstly, the transfer needs to be necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and secondly, the receiving authority should be responsible for these tasks. Thirdly, the providing member state needs to have given its consent. Fourthly, the third state or body needs to ensure an adequate level of data protection. The latter can however be derogated from.

The content of the instrument is on several aspects rather disappointing from a data protection point of view. With regard to the quality of the processing of personal data, the applicable provisions have been widely formulated and seem to aim for purpose deviation rather than purpose limitation (De Busser, 2009a, p. 163-201). With regard to the transfer to third states or institutions, the adopted provisions confirm the incoherence in the judicial and law enforcement cooperation in criminal matters between the EU member states on the one hand and third states or institutions on the other hand.

This incoherence is substantiated by means of three aspects of the framework decision: the limited weight that is attached to the adequacy requirement, the limited scope of the instrument and the effect that the framework decision has on existing and future provisions on data transfers to third states and institutions.

4.1 The weight of the adequacy requirement in the framework decision

Article 13 of the framework decision on the transfer to competent authorities in third states or to international bodies provides that the third state or international body concerned ensures an adequate level of protection for the intended data processing. Nevertheless, more requirements – that cumulatively need to be fulfilled – apply.

Earlier drafts of the provisions on the transfer to third states and bodies included the requirement of consent by the transmitting member state or authority as the only requirement to be fulfilled (Council, 7215/07, 13 March 2007). The Council however paid attention to the remarks made by the European Data Protection Supervisor and raised the conditions to a level much more in line with the provisions of the additional protocol (EDPS, *O.J.C*, 23 June 2007, issue 139, § 27-28). Consent of the state from which the data were obtained was made one of the four conditions to be fulfilled subject to derogations. The other two conditions include the purpose of the exchange for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the responsibility of the receiving authority or body for these tasks.

Not responding to the concerns of the EDPS, the framework decision does not encompass more detailed indications of how to – uniformly – assess the adequacy of a state's data protection legislation, than the circumstances given by the additional protocol to the data protection convention.

Similarly, the lawful derogations from the adequacy requirement are a copy of the latter. Based on its origin in the additional protocol the legitimate prevailing interests should refer to article 8, § 2 of the ECHR and article 9, §2 of the data protection convention, including state security, public safety, health and morals and the economic well-being of the state. Obviously, these leave plenty of room for more specific interests of the state to fit in one category or the other. Specifically the interests of state security can – nevertheless legitimate and prevailing – cause a shift of personal data gathered for criminal purposes to use for administrative purposes. This can be done while jumping over the requirement of an adequacy check, thus releasing the data into a legal system of which the data protection provisions are possibly not adequate in comparison to the EU standards. This provision in particular is in need of more clarification by means of an exhaustive list, a supervisory authority that judges the legitimacy and the prevailing force of a specific interest or by laying down standards on when to consider an interest as prevailing over the adequacy check of a data protection system.

As a copy of the additional protocol to the data protection convention, the comment that these derogations are broadly formulated is equally valid for the framework decision as well as for the protocol. Nevertheless, the protocol is in general applicable to all automatic data processing and was not designed to protect personal data in criminal matters. Furthermore, where the states ratifying the additional protocol are bound to provide in the adequacy requirement, they have the discretion to determine derogations to the rule. Therefore, implementing the principles from the protocol in criminal matters, the derogations of the protocol leave too much room for avoiding the adequacy assessment. Particularly since the significance of purpose limitation is considered as one of the basic data protection principles supported by the EU and encompassed by an adequate level of data protection, the use of these derogations can have wide-ranging implications.

Thus, the structure and content of article 13 of the framework decision is not new, neither surprising. What is surprising, however, is the fact that these provisions are limited to data transmitted or made available by a member state to another member in order to transfer them to a third state or body. It is therefore not aimed at, neither does it include, data that were gathered by the transmitting member state itself.

Together with the effects of the framework decision on the existing and future provisions on outgoing data transfers, the content of article 13 results in anything but a substantial adequacy requirement for the third pillar.

4.2 The scope of the framework decision

The formal scope of the framework decision is identical to the Directive 95/46/EC as it includes the processing of data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system (article 1, §3). The definition of 'filing system' is evidently identical to the one included in the Directive.

The material scope however, covers a part of the exceptions in article 3 §2 of the Directive and has been delineated by means of a functional criterion. Instead of delineating the authorities that are or are not included, for example law enforcement authorities or judicial authorities, the competent authorities are defined by Title VI of the TEU and the authorities that are authorized by national law to process personal data within the scope of the framework decision (article 2, h). This refers to authorities that are competent to process personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Which activities are exactly included in the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, is not provided by the definitions of the framework decision. Nevertheless, the link with criminal offences ensures that also the processing of personal data proactively can be included.

After elaborate discussions the Council decided to limit the Framework Decision to cross-border exchange of personal data and not include domestic exchange (Council (Justice and Home Affairs), 12604/07, 18 September 2007 and EDPS, Press release, 20 September 2007, www.edps.europa.eu). The resistance of a number of member states – lead by the United Kingdom – to the application of the framework decision to domestic data processing, finally made the Council give up on its original scope as no consensus would be reached (Council, 12154/07, 4 September 2007, p. 2 and Peers, 2007, p. 2).

This means that data that have been collected by the member states' authorities do not fall within the scope of the framework decisions and thus are not subjected to the adequacy requirement when this member state transfers the data to a third state or body. Instead, the transfer of these data is subjected to national law. Only in case the member state concerned has ratified the additional protocol to the data protection convention or has included the adequacy requirement through an implementation of Directive 95/46/EC in criminal matters, should the adequacy requirement be applied to the outgoing data transfers.

Therefore, the framework decision creates a discrimination between the personal data that have been collected by the member state and the personal data that have been transferred or made available by another member state. Data included in criminal investigation files can consist partially of nationally gathered data and partially of received data. When data from the file are requested for the purpose of a criminal investigation or procedure in a third state, the data that are included in the file have to be distinguished regarding their origin. Thus, data in the same file can be subjected to two different sets of data protection rules. In case the receiving criminal justice system is evaluated as being inadequate, the nationally gathered data of the same file can be exchanged where the received data can not.

This distinction could even create grounds for an evaluation of the framework decision by the Court of Justice by means of a prejudicial question and the competence of the Court to rule upon the validity of framework decisions (article 35, §1 TEU). By analogy with the case brought before the Belgian Constitutional Court by the non-profit organization 'Advocaten voor de Wereld' regarding the European Arrest Warrant, the framework decision on data protection in criminal matters could be judged on this discriminatory aspect (Court of Justice, C-303/05, 3 May 2007). Because the distinction made between nationally gathered data and data received or made available by another member state is not objectively justified, the Constitutional Court could refer the case to the Court of Justice. In the case regarding the European Arrest Warrant, the relevant difference – requirement of double criminality for all offences not included in the list in framework decision on the European Arrest Warrant – was according to the Court objectively justified due to the seriousness of the offences included in the list.

A distinction based on objective aspects of the data cannot be made with regard to the personal data gathered nationally or received from another member state. On the contrary, limiting the scope of the framework decision was a choice inspired by national policy. Applying the instrument only to cross-border exchange was the adamant position of '*a substantial number of delegations*' of the member states (Council, 12154/07, 4 September 2007).

4.3 Effects of the framework decision on existing and future provisions

Similar to the instruments applicable on data exchange between member states, the entry into force of the framework decision on data protection in criminal matters also has significant effects on the instruments on the exchange of personal data with third states.

Article 26 of the framework decision lays down the general rule that existing bilateral and multilateral agreements between the member states or the Union on the one hand and third states on the other hand, are unaffected by the framework decision. Future agreements should comply with the new instrument, specifically with article 13 on transfers to third states and international bodies. This particular article will nevertheless also play an important part in the existing bi- and multilateral agreements as the requirement of consent in the provision – §1, c) or §2 as appropriate – must be applied to these agreements as well.

The already concluded instruments will still be applicable in their original form, even though with the addition of a consent requirement. This means that no agreements need to be renegotiated and obtained clauses will remain in force. Besides the

significance for the political ties that the member states as well as the Union have built up with third states, legal certainty is ensured by not touching acquired rights and obligations after the adoption of the framework decision. The addition of the consent requirement means that with regard to the concluded data exchange by virtue of existing bi- and multilateral instruments, the member state that supplied the data now also needs to give its consent for the transfer to the third state. However, the requirement can be derogated from in cases in which the consent cannot be obtained in good time and the transfer is essential. The necessity is motivated by the prevention of an immediate and serious threat to public security of a member state or third state or to essential interests of a member state. Due to the width of this derogation, the consent requirement is thus not the type of additional requirement that would impede the functioning of an already existing agreement. Therefore, the relationships of data exchange with third states that are effective at the time of the entry into force of the framework decision are secured.

The requirement of ensuring an adequate level of data protection remains untouched where it has been included in existing agreements. As mentioned before, the requirement has not been included in all legal instruments related to data exchange in criminal matters.

Also unaffected by the framework decision, is the additional protocol to the data protection convention. This means that the adequacy requirement the ratifying states are bound by in their data exchange with states not bound by the data protection convention, stays afloat pursuant to recital 41 of the preamble.

Important to note is that article 26 of the framework decision explicitly refers to 'obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision'. Consequently, it is not necessary for the agreements to have entered into force then. The obligations or commitments merely need to 'exist', which is a legally vague and undefined term. As obligations or commitments cannot exist without the agreement being concluded, it would have been a much clearer rule to include the prerequisite of a signed agreement.

By only including member states and the Union, this means that the agreements concluded between Europol or Eurojust on the one hand and third states on the other hand, are not encompassed by the rule in article 26. Thus, these remain unaffected in their existing as well as in their future agreements with third states.

5 The future of adequacy: from Vienna to Stockholm via Washington

The history of the adequacy requirement dates back to the creation of the internal market and the aforementioned Directive 95/46/EC. In criminal matters it has not been made a generally binding prerequisite for outgoing transfers of personal data. Recent developments have shown that this is not likely to happen in the future, even though significant efforts have been made to create a data protection framework for the third pillar. Nevertheless, in the judicial and law enforcement cooperation in criminal matters between the EU, Eurojust and Europol on the one hand and the US on the other hand, the adequacy requirement has become discredited.

5.1 From Vienna to the Hague

The first call for a harmonisation of data protection rules under the title of judicial and police cooperation in criminal matters was made in the Vienna Action Plan in 1998 (*O.J.C* 23 January 1999, issue 19, § 7 and § 47). Even though these plans were accompanied by an Italian initiative covering the same ideas on harmonising data protection in the third pillar, the first attempts to develop a legal instrument on data protection in criminal matters failed.

After the European Council refreshed the Council and the Commission's memory in the Hague Programme, an Action Plan was set up to submit proposals for ensuring 'adequate safeguards and effective legal remedies for the transfer of personal data for the purpose of police and judicial cooperation in criminal matters'. The new proposal drafted by the Commission in 2005 (Commission, COM(2005) 475 final, 4 October 2005), failed to resolve a number of crucial questions. A new proposal was therefore presented by the German presidency in April 2007 (Council, 7315/1/07, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 24 April 2007). Nevertheless, the adequacy requirement did not undergo significant changes in these proposals. With the exception of the draft proposal of March 2007 where briefly the consent requirement was included as the only condition for making outgoing personal data transfers in criminal matters. In the following draft text the adequacy requirement was already restored in its former configuration as one of the conditions to be fulfilled.

Notwithstanding the current structure of the article on outgoing data transfers, the three aspects as examined above demonstrate that the adequacy requirement as it is included in the new framework decision does not entirely suit data protection in international cooperation in criminal matters to the best of its abilities. Looking at the manner in which the adequacy requirement is used in agreements with third states that cover data transfers in criminal matters, the picture is equally alarming concerning the transatlantic cooperation.

5.2 The transatlantic journey

The cooperation in criminal matters between the EU and the US earns a specific spot in the discussion on the adequacy requirement. Before the conclusion of the 2003 agreement on mutual legal assistance in criminal matters between the EU and the US, the cooperation between judicial and law enforcement authorities in criminal matters was regulated by bilateral mutual legal assistance treaties (MLATs). None of these MLATs include the adequacy requirement. The entry into force of the 2003 mutual legal assistance agreement could have changed this as new bilateral instruments needed to be developed in order to interpret the existing MLATs in the light of the agreement.

Research has shown that the American system of data protection in criminal matters is as such not fully compatible with the EU standards on data protection. The lack of generally binding rules on purpose limitation and data retention combined with the tradition of data sharing amongst government agencies, result in a data protection landscape that is too divergent from the EU legislation to be labelled as adequate with-

out guaranteeing additional safeguards (De Busser, 2009a, p. 175-191. Regarding the differences between both systems see also Whitman, 2004, p. 1151-1221 and Harris, 2007, p. 796-799). Nevertheless, this did not withhold Europol, Eurojust and the EU from concluding agreements covering the exchange of personal data with the US authorities.

5.3 Adequate transatlantic alliances in the future?

Approaching the end of the Hague Programme in 2010, the German presidency set up two informal working groups at ministerial level to discuss a successive plan on the future of European area of freedom, security and justice. The Informal High Level Advisory Group on the Future of European Home Affairs Policy (Future Group Home Affairs) on the one hand and the High-Level Advisory Group on the Future of European Justice Policy (Future Group Justice) on the other hand, considered the main challenges the EU would face in the period 2010-2014. These preparations would lead to the new Stockholm programme, the successor to the Hague plan that should be concluded during the Swedish presidency in the fall of 2009 (Vermeulen, 2009).

At that given time, the Council discussed the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and due to the focus on information exchange in the Hague Programme, the subject of data protection received much attention in both reports. The report of the Future Group on Justice continued largely along the data protection lines the EU had set out before. Introducing new ideas on transatlantic cooperation, including convergence of the different legal frameworks of data protection, the Future Group makes the assumption that the US endorses a data protection system that is compatible with the EU's data protection regime. The Group goes as far as having a strong statement registered on a 'Euro-Atlantic of cooperation with the United States in the field of Freedom, Security and Justice'. This implies an intense cooperation with a criminal justice system that is still fundamentally different from the EU's criminal justice systems. In the preparatory report by the Future Group on Home Affairs already politically departed from the assumption that the US criminal justice system, including its data protection system, is sufficiently compatible to organize the same type of cooperation that exists between EU member states in the relations with the US. This means that the adequacy of the US data protection system is merely assumed, rather than thoroughly examined.

The Future Group introduced the concept of a *Euro-Atlantic area* of cooperation with the US in the field of freedom, security and justice. The Group hereby believes that the same principles that are applicable in the cooperation between EU member states, can be copied to the EU-US cooperation (Vermeulen, 2009). This would imply the application of the principle of mutual recognition to the EU-US relations. The basic conditions for mutual recognition – mutual trust and common minimum standards – are thus equally assumed, rather than thoroughly examined. In addition, these prerequisites for the principle of mutual recognition are not necessarily fulfilled in the internal cooperation between EU member states (Vernimmen-Van Tiggelen and Surano, 2008). As stated above, the current state of the art shows that the US are not compatible on a data protection level with the EU, even though the Future Group's reasoning was based on compatibility between both systems.

Chapter 2.3 of the Stockholm programme ends in a similar reasoning, by stating that the EU – US cooperation on data protection could serve as a basis for future Agreements. Taking a closer look at the content of Chapter 2.3 on protection of personal data and privacy, two statements are particularly eye-catching. On the one hand the Chapter highlights the need for a comprehensive protection scheme covering all areas of EU competence. On the other hand the Chapter ends with an impressive statement that bilateral and multilateral instruments could be based on the example of the EU – US cooperation in data protection. Based on these statements, one could reason that the EU's internal data protection is in need of improvement as basic principles need to be restated whereas the data protection in its transatlantic relations should serve as *an example* for international standards on data protection. The combination of these two statements included in the Stockholm Programme amounts to a glorification of the Agreements concluded between the EU and the US on the exchange of personal data.

In view of the research set out above, the word 'example' is a strong and rather inappropriate word to use in this context. In order to use it rightfully the basic standards of data protection applicable in the EU should have been complied with in the cooperation with the US on data protection. Earlier research has proven that this is not entirely the case (De Busser, 2009a, p. 175-191). The essential element of the (application of the) adequacy requirement has also been examined in the transatlantic relations in criminal matters and resulted in a similar negative answer. The adequacy requirement is not consistently applied in the EU's law enforcement and judicial cooperation in criminal matters with third states.

According to the Stockholm Programme the '*Union must be a driving force behind the development and promotion of international standards for personal data protection and in the conclusion of appropriate bilateral or multilateral instruments. The work on data protection conducted with the United States could serve as a basis for future Agreements.*' The question whether the EU – US cooperation in criminal matters should serve as a role model for data protection, should be answered in a negative manner. Without a solid check of possible inconsistencies between the EU level of data protection and the level of data protection of the US, personal data can now be transferred with American law enforcement and judicial authorities and be fairly effortlessly shared with other agencies in the US. If this picture would function as an example for future bilateral and multilateral Agreements with other states, the data protection standards laid down by the widely ratified data protection Convention will be breached by a number of states. If this cooperation implying the elimination of the adequacy requirement would function as an example for future bilateral and multilateral Agreements, the additional protocol to the data protection Convention loses its meaning.

Obviously not every third state will apply specific rather than general rules on data protection and not every third state has a tradition of data sharing, encouraging the creation of Agreements based on the example of the Europol – US Agreement, the Eurojust – US Agreement and the EU – US Agreement, is not consistent with the idea of a stronger framework of data protection.

6 Conclusion: coherency with a twist

The adequacy requirement is not a general condition for data transmission, which is an out of the ordinary way of working in criminal matters. Coherency is traditionally the key word in the third pillar due to the risk of *forum shopping*. In the case of personal data exchange, an incoherent data protection policy would potentially result in *data shopping*. Furthermore, it could result in cross-pillar data shopping when the adequacy requirement is not uniformly applied in the first and third pillar. The reality of purpose deviation in the EU's legal instruments intensifies this concern.

Due to the sensitivity of judicial and police cooperation in criminal matters, especially in cooperation with third states or institutions, it is at all times advisable to allow for a common attitude towards sending personal data with a view to inserting them in a criminal procedure. More specifically, a common attitude in protecting the use of the personal data after they have been transmitted – the adequacy requirement – is necessary in order to effectively protect our own EU standards. Independent from the question whether the EU lives up to its own standards, the data protection rules the EU lays down are thus not satisfactorily safeguarded in the cooperation with third states or institutions.

Furthermore, the differences between the assessment involved in fulfilling the adequacy requirement as implemented by Eurojust and Europol, add to the diversity of a safeguard that should protect all personal data originating from the EU.

With Eurojust, Europol and the national data protection regulations being excluded from the scope of the new framework decision on data protection in criminal matters, this instrument has only added to the lack of coherency in this field. The same instrument has provided in the adequacy requirement but failed to make this a strong prerequisite in the relations with third states or institutions by including derogations that can be fairly effortlessly used to circumvent the assessment of an adequate level of data protection.

Nevertheless, even when an adequate level of data protection is laid down as a *conditio sine qua non*, it is not always applied. The agreements the US concluded with Europol and Eurojust are good examples. In particular because this requirement was complied with in the relations with other third states, increases incoherency. Both Europol and Eurojust support more lenient standards in their cooperation with the US than in their cooperation with other third states. The US was in fact labeled as supporting an adequate level of data protection, where the necessary confirmation for this label was not provided and cannot be provided.

Data protection provisions in future agreements with other third states could potentially suffer when the new partners in the negotiation demand the same lenient rules from Europol or Eurojust in order to obtain an easier exchange of data.

The EU has not developed cooperation agreements of the same type with any other third states, but was equally accommodating to the US in pushing aside the adequacy requirement. This equally weakens the position of the EU to demand compliance with its data protection standards in future agreements of this type. The risk of negotiating basic data protection rules in the cooperation with third states and institutions thus increases when no coherent policy is developed on the protection of the EU's data protection standards in outgoing data exchange.

In the future plans for developing further cooperation with third states, the trend continues. Especially with regard to the transatlantic cooperation, the label of an adequate partner for cooperation in criminal matters is strong. So strong that plans for a Euro-Atlantic zone of cooperation have surfaced in which the cooperation with the US would run along the same lines as the cooperation between the EU member states. Disregarding the basic principles required for this type of cooperation and the fact that their fulfilment is equally within the EU incomplete, does not bode well for the coherency of future policy plans for judicial and law enforcement cooperation in criminal matters.

There is thus a significant need for a common attitude on the requirement of an adequate level of data protection within the EU as well as in the EU's relations with third states and institutions.

Regardless of the EU pillar that encompasses the specific exchange of personal data, the adequacy requirement should be applied by all member states and by the EU institutions and the EU itself in their relations with third states, including the US. Ensuring coherency means a genuine assessment of the adequacy of the third state's data protection level rather than rubber stamping a state as being adequate without thorough evaluation. Ensuring coherency also means developing a common assessment method, equally in a cross-pillar fashion. This common attitude should equally be sustained regardless of the fact whether the exchange of personal data encompasses the exchange of domestically gathered data or data received or made available by another member state. However, it is clear that the more recent legal instruments covering judicial and law enforcement data exchange between the EU member states and in the transatlantic cooperation in criminal matters as well as the most recent framework decision on data protection in criminal matters, do not answer to this need for coherency.

7 Bibliography

Policy and legal documents

Council of Europe

European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS N° 5, 4 November 1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS N° 108, 28 January 1981

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, ETS N° 181, 8 November 2001

European Union

95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L, 23 November 1995, issue 281, p. 31-50.

Council, Council Act adopting the rules on the transmission of personal data by Europol to third states and third bodies, O.J.C, 30 March 1999, issue 88, p. 1-3.

European Parliament and Council, Regulation (EC) no. 1073/1999, 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), O.J.L 31 May 1999, issue 136, 1-7.

Commission, Decision no. 1999/352/EC, ECSC, Euratom, 28 April 1999 establishing the European Anti-fraud Office (OLAF), O.J.L 31 May 1999, issue 136, 20-22.

Safe Harbour Privacy Principles issued by the U.S. Department of Commerce, July 21, 2000, www.export.gov/safeharbor/ SHPRINCIPLESFINAL. Htm

Europol JSB, Opinion in respect of the data protection level in the United States of America, Document 01/38, 26 November 2001.

Agreement between the United States of America and the European Police Office, 6 December 2001, www.europol.europa.eu

European Parliament and Council, Regulation 45/2001 on data exchange between Community institutions or bodies or to third institutions or bodies, O.J.L, 12 January 2001, issue 8, p. 1-22.

Council, 6316/2/01, Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union, 12 April 2001.

European Parliament and Council, Directive 2002/58/EC on data processing in the telecommunication sector, O.J.L, 31 July 2002, issue 201, p. 37-47.

Council, Informal explanatory note regarding the draft supplemental agreement between the United States of America and the European Police Office on the exchange of personal data and related information, 13696/1/02, 28 November 2002.

Council, Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, O.J.C, 6 June 2002, issue 63, p. 1-13.

Council, Exchange of letters related to the Supplemental Agreement between the United States of America and Europol on the exchange of personal data and related information, 13996/02, 11 November 2002

Supplemental Agreement 20 December 2002 between the United States of America and Europol on the exchange of personal data and related information, www.europol.europa.eu.

Council, Agreement 25 June 2003 on mutual legal assistance between the European Union and the United States of America, O.J.L 19 July 2003, issue 181, p. 34-42

Commission of the European Communities, Commission Decision 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, O.J. L, 6 July 2004, issue 235

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

Commission, COM(2005) 597 final, Communication from the Commission 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, 24 November 2005.

European Parliament and Council, Directive no. 2006/24/EC, 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, O.J.L 13 April 2006, issue 105, p. 54-63.

European Data Protection Supervisor, Opinion 20 January 2006 on the 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), O.J.C 25 April 2006, issue 97, p. 6-10.

Council, 13738/06, Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States Of America, Concerning the Interpretation of Certain Provisions of the Undertakings Issued by DHS on 11 May 2004 in Connection with the Transfer by Air Carriers of Passenger Name Record (PNR) Data, 11 October 2006.

Agreement between Eurojust and the United States of America, 6 November 2006, www.eurojust.europa.eu

Council, Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II), 14914/06, 12 December 2006.

Council, 7315/1/07, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 24 April 2007.

Council, 11004/07, Draft Conclusions on access to Eurodac by Member State police and law enforcement authorities as well as Europol, 19 June 2007.

Council, 11004/07 Cor 1, Draft Conclusions on access to Eurodac by Member State police and law enforcement authorities as well as Europol, 2 July 2007.

Council, Council Decision of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J. L, 4 August 2007, issue 204, p. 16-17.

Council Decision no. 2007/533/JHA, 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), O.J.L 7 August 2007, issue 205, p. 63-84.

Standing Committee of Experts on International Immigration, Refugee and Criminal law, CM0712-IV, 18 September 2007, www.commissie-meijers.nl.

Standing Committee of Experts on International Immigration, Refugee and Criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, 18 September 2007.

European Data Protection Supervisor, Third opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. C 139, 23 June 2007, p. 1-10.

The Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), Report, Freedom, Security, Privacy – European Home Affairs in an Open World, June 2008 and High-Level Advisory Group on the Future of European Justice Policy, Proposed Solutions for the Future EU Justice Programme, June 2008.

Council, 9831/08, EU US Summit, 12 June 2008 – Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, 28 May 2008.

Council, Decision no. 2008/633/JHA, 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, O.J.L 13 August 2008, issue 218, p. 129-136.

Practical Agreement on arrangements of cooperation between Eurojust and OLAF, 24 September 2008, www.eurojust. europa.eu/official_documents /eju_agreements. htm.

European Data Protection Supervisor, Press Release 11 November 2008, Opinion on transatlantic information sharing for law enforcement purposes: Progress is welcomed, but additional work is needed, p. 13, www.edps.europa.eu.

Council, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L 30 December 2008, issue 350, p. 60-71.

Communication from the Commission to the European Parliament and the Council, an area of freedom, security and justice serving the citizen, COM (2009) 262/4.

United States

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot Act), Public Law 107-56, October 26 2001

Department of Justice, Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, Pursuant to Public Law 106-544, Section 7, 13 May 2002, p. 7, www.justice.gov/archive/olp/rpt_to_congress.pdf

Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law, 108-458, 17 December 2004

Department of Justice, Overview of the Privacy Act of 1974, 2004 edition, www.usdoj.gov/oip/04_7_1.html

DOYLE, C., Administrative subpoenas in criminal investigations: a sketch, CRS Report for Congress, 17 March 2006, http://ftp.fas.org/sgp/crs/intel/RS 22407.pdf.

DOYLE, C., National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, CRS Report for Congress, 28 March 2008, p. 1-5, www.fas.org/sgp/crs/intel /RL33320.pdf.

Literature

BANISAR, D. and DAVIES, S., "Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments", J. Marshall J. Computer & Info. L. 1999, Vol. 18, no. 1, p. 3-111.

BENNET, C.J. and RAAB, C.D., "The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response", The Information Society 1997, Vol. 13, p. 245 – 263.

BOEHMER R.G. and PALMER, T.S., "The 1992 EC Data Protection Proposal: an Examination of it Implications for the US Business and the US Privacy Law", American Business Law Journal 1993, Vol. 31, p. 265-311.

BYGRAVE, L.A., Data protection law. Approaching its rationale, logic and limits, 2002, The Hague-London-New York: Kluwer law International.

CIOCCHETTI, C.A., "The future of privacy policies: a privacy nutrition label filled with fair information practices", John Marshall Journal of Computer and Information Law 2008, p. 1-45.

DE BUSSER, E., Data protection in EU and US criminal cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities, Antwerp-Apeldoorn, Maklu, 2009 (forthcoming).

DE BUSSER, E., 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day', in Marc Cools et.al., Readings on Criminal Justice Criminal Law & Policing, GOFS Research Paper Series, Antwerp-Apeldoorn, Maklu, 2009, p. 163-201.

DE HERT, P. (ed.), Privacy en Persoonsgegevens, Brussels, Politeia, 2004, (loose-leaf).

DE HERT, P. and DE SCHUTTER, B., "International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift" in MARTENCZUK, B. and VAN THIEL, S. (eds.), Justice, Liberty, Security: New Challenges for EU External Relations, VUB Press, Brussels, 2008, (I.E.S. series nr. 11), p. 299-335.

DONAHUE, L.K., "Anglo-American Privacy and Surveillance", J. Crim. L. & Criminology 2006, Vol. 96, p. 1059-1208.

HARRIS, E.C., "Personal data privacy tradeoffs and how a Swedish church lady, Austrian public radio employees, and transatlantic air carriers show that Europe does not have the answers", American University International Law Review 2007, p. 745-799.

LEVIN, A. and NICHOLSON, M.J., "Privacy law in the United States, the EU and Canada: the allure of the middle ground", UOLTJ 2005, p. 357-395.

LONG, W.J. and QUEK (2002), M.P. Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise, Journal of European Public Policy, Vol. 9, Issue 3, p. 325-344.

VERMEULEN, G., Transatlantisch monsterverbond of verstandshuwelijk?, Panopticon, 2004, p. 96-103.

VERMEULEN, G., Stockholm richting toekomst, via Brussel, Politie, justitie en strafrecht in de Europese Unie, episode 2010-2014, Panopticon, 2009, (forthcoming).

VERVAELE, J.A.E., "Gegevensuitwisseling en terrorismebestrijding in de VS en Nederland: emergency criminal law?", Panopticon 2005, p. 27-52.

WHITMAN, J.Q., "The two western cultures of privacy: dignity versus liberty", Yale Law Journal 2004, p. 1151-1252.

Case law

ECtHR, Leander v. Sweden, 1987.

ECtHR, Rotaru v Romania, 2000.