Utrecht Law Review published by igitur

EU data protection in transatlantic cooperation in criminal matters
Will the EU be serving its citizens an American meal?

Els De Busser*

1. Introduction

In June 2009 all eyes were on the European Commission which was about to come up with a communication on a new five-year plan (2010-2014) for justice and home affairs, the so-called Stockholm Programme.[1] Subsequently, a draft document was published in October 2009, which will be adopted by the EU Heads of State and Government in December 2009.[2] The successor plan for the well known Hague Programme was highly anticipated after it was prepared several months earlier by two – instead of the traditional one – working groups. The 'High-Level Advisory Group on the Future of European Justice Policy' (hereafter: the Future Group on Justice) and the 'High Level Advisory Group on the Future of European Home Affairs Policy' (hereafter: the Future Group on Home Affairs) each issued its report in June 2008.[3]

As the Council was busy discussing the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereafter: Framework Decision on data protection in criminal matters)[4] and due to the focus on information exchange in the Hague Programme, the subject of data protection received a great deal of attention in both reports. The report of the Future Group on Justice continued largely along the same data protection lines as the EU had previously set out. The report of the Future Group on Home Affairs introduced new ideas on cooperation with the US, including a greater convergence of the different legal frameworks of data protection. The Future Group thus makes the assumption that the US endorses a data protection system that is compatible with the EU's data protection regime and that both can converge together. This idea is taken one step further and the Group makes a strong statement on a 'Euro-Atlantic cooperation with the United States in the field of Freedom, Security and Justice'.[5] This implies an intense cooperation with a criminal justice system that is still fundamentally different from the EU's criminal justice systems.

Gradually, the tone of these statements has softened in the documents that were published after the preparatory work of the two Future Groups. The communication that incorporated the

* Dr Els De Busser is currently a researcher at the Max Planck Institut für ausländisches und internationales Strafrecht, Freiburg (Germany), European Criminal Law section, email: e.busser@mpicc.de

1 COM(2009) 263/4.

2 14449/09 16 October 2009.

3 *High-Level Advisory Group on the Future of European Justice Policy*, June 2008 and *Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group')*, June 2008.

4 Framework Decision 2008/977/JHA, *OJ* L 350, 30.12.2008, pp. 60-71.

5 *Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group')*, June 2008, Para. 50.

first draft of the Stockholm Programme (hereafter: the communication) includes a Chapter 2.3 that ends with a similar reasoning as the aforementioned statement by the Future Group, by stating that 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 the protection of personal data and privacy in the communication, two statements particularly catch the eye. 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 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 included statements almost sounds like a glorification of the agreements concluded between the EU and the US on the exchange of personal data.

In the published draft of October 2009 (hereafter: the draft Stockholm Programme) the chapter on the protection of personal data and privacy is much more mitigated. Especially deleting the statement on using EU-US cooperation in data protection as an example was a step in the right direction. Nevertheless, the inclusion of the statement in the communication deserves a closer look.

In this contribution, first the need for a new legal framework on data protection will be studied in order to assess whether this call for a comprehensive protection scheme is justified. Secondly, a review will be made of the data protection provisions in the transatlantic agreements concluded in the field of criminal matters. This will demonstrate the implications of considering these agreements as examples for future bilateral and multilateral agreements in the communication.

2. A comprehensive protection scheme should be introduced covering all areas of EU competence

Chapter 2.3 of the communication on the Stockholm Programme explicitly states that a comprehensive protection scheme should be introduced. This is a statement that is further 'clarified' in the list of priority issues which provides that the EU must establish a comprehensive personal data protection scheme covering all areas of EU competence. The statement remained in the draft Stockholm Programme.

Stating that a comprehensive protection scheme should be introduced in all areas of EU competence can imply two things: either no protection scheme exists, or the existing scheme is not comprehensive and thus does not cover all areas of EU competence.

Concluding whether or not a comprehensive system of data protection exists can only be done after examining two aspects. The data protection model that the EU endorses should first be examined as this model can vary and thus influence the scope of the applicable rules, their enforcement, their efficiency and their effectiveness. Secondly, the material scope of the applicable system will be studied in order to conclude whether the system covers all or only some areas of EU competence.

2.1. Data protection model

Research on privacy protection has identified four different models for safeguarding personal data.[6] In order to protect personal data, states use general comprehensive laws, sector-specific laws, self-regulation by companies and/or privacy enhancing technologies.

First, general laws that have a wide-ranging scope and include standards on data protection. An excellent example is the 1981 Council of Europe (hereafter: CoE) Convention for the protection of individuals with regard to automatic processing of personal data (hereafter: Data Protection Convention).[7] The instrument's scope encompasses all automatic processing of all types of personal data gathered in the public as well as the private sector, including, for example, commercial, financial, criminal, medical or educational matters. It covers standards on personal data as such, standards on the collection, use and dissemination of data, transborder data flows and rules on mutual assistance between states and is thus a typical comprehensive data protection instrument.[8]

This umbrella Convention has been ratified by all Member States of the EU and thus functions as the mother instrument on data protection for the EU Member States, but is not an EU instrument as such.

Laws on data protection that are applicable to specific sectors have the advantage of including custom-made provisions that have been adjusted to fit the special needs of data processing in a certain sector. Regulation (EC) 45/2001 creates a set of data protection rules that have been tailored to the processing of personal data by Community institutions and could thus be labelled as a sector-specific instrument.[9] Still, the regulation needs to comply with the general standards that have been laid down in the mother Convention of 1981 which covers all automatic processing of data. The Regulation however broadened its scope to also include partly automatic and non-automatic means of processing.

The third data protection model for industry self-regulation takes one step further in the tailor-made approach and allows companies to develop their own data protection systems in the shape of codes of practice. This system is flexible, inexpensive but weak in enforcement.[10] Privacy technologies finally enable the internet user to safeguard his or her own data processing by applying certain programs and systems such as encryption.[11]

Many states – or groups of states like the EU – will use a combination of several models.[12] The EU applies a combination of comprehensive legislation and sectoral laws. The US applies a combination of sectoral laws, industry self-regulation and privacy enhancing technologies.[13]

2.2. Comprehensive data protection

Which characteristics make a protection scheme a comprehensive one? It is not necessary for a comprehensive data protection scheme to consist of one legal instrument. However, the provi-

---

6 D. Banisar & S. Davies, 'Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments', 1999 *J. Marshall J. Computer & Info. L.* 18, no. 1, pp. 13-14 and W.J. Long & M.P. Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise', 2002 *Journal of European Public Policy* 9, no. 3, p. 330.

7 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, *ETS*, no. 108.

8 See also D. Banisar & S. Davies, 'Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments', 1999 *J. Marshall J. Computer & Info. L.* 18, no. 1, p. 14.

9 Regulation (EC) no. 45/2001, *OJ* L 8, 12.1.2001, pp. 1-22.

10 D. Banisar & S. Davies, 'Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments', 1999 *J. Marshall J. Computer & Info. L.* 18, no. 1, p. 10 and W.J. Long & M.P. Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise', 2002 *Journal of European Public Policy* 9, no. 3, p. 330.

11 D. Banisar & S. Davies, 'Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments', 1999 *J. Marshall J. Computer & Info. L.* 18, no. 1, p. 10.

12 *Ibid.*, p. 9.

13 See also E. De Busser, *Data protection in EU-US criminal cooperation*, 2009, pp. 235-248.

sions on data protection – possibly spread over several instruments – should cover all types of data processing and they should be consistent with each other.[14]

Under the current pillar structure of the EU, it is not possible to introduce one legal framework covering data protection even though the basic text is a single convention on data protection enacted by the CoE.[15]

Data protection in the EU's first pillar is currently regulated by three instruments: Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,[16] Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[17] and Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector.[18] Data protection in the EU's third pillar is regulated by the new Framework Decision on data protection in criminal matters. With the entry into force of the Lisbon Treaty and the subsequent disappearance of the traditional pillar structure, a single legal framework applying to all data processing in all areas of EU competence becomes a genuine possibility.[19] However, this would imply replacing the existing instruments that have been tailor-made for specific sectors in which personal data are processed. Regardless of the Lisbon Treaty and the pillar structure, however, it was possible as well as essential to ensure consistency between the legal instruments on data protection.

Consistency between the data protection provisions is a crucial element of a comprehensive protection scheme. Unfortunately, consistency was not the legislator's first consideration when drafting the Framework Decision on data protection in criminal matters.

Both the legal framework and the data protection standards that are laid down by it are studied here first. This is followed by a closer look at the consistency of the data protection provisions in these instruments. These steps are necessary in order to reach a conclusion on the need for a comprehensive data protection scheme.

2.2.1. Legal framework covering all types of data processing

The CoE Data Protection Convention is a comprehensive instrument. Its scope is general and it includes all automatic data processing in the private as well as in the public sector, including commercial, financial, educational and other types of data. Thus, it can also be applied to data processing in criminal matters provided that proper attention is given to the specific characteristics of personal data processed in criminal matters relating to the right to a fair trial.

In addition, the Data Protection Convention is the basic set of data protection rules which are often referred to by the legal instruments governing cooperation in criminal matters. The Europol Convention[20] and the Europol Decision[21] that will soon replace it, both explicitly refer to the Data Protection Convention when laying down standards on data protection. The Schengen

14 *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July 2009, Para. 28.
15 *Ibid.*, Para. 27.
16 Directive 95/46/EC, *OJ* L 281, 23.11.1995, pp. 31-50.
17 Regulation (EC) no. 45/2001, *OJ* L 8, 12.1.2001, pp. 1-22.
18 Directive 2002/58/EC, *OJ* L 201, 31.7.2002, pp. 37-47 amended by Directive 2006/24/EC, *OJ* L 105, 13.4.2006, pp. 54-63.
19 *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July 2009, Para. 27.
20 Convention 26 July 1995 based on Art. K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *OJ* C 316, 27.11.1995, pp. 2-32.
21 Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ* L 121, 15.5.2009, pp. 37-66.

Implementation Convention,[22] the Prüm Convention[23] and the Benelux Police Cooperation Convention[24] all include similar references.

As the basic binding legal instrument for data protection for the EU Member States which have all ratified it, the Convention lays down the five crucial requirements that personal data should abide by in order to constitute quality data undergoing automatic processing. Article 5 of this Convention – modelled on the basic standards for data protection presented by earlier enacted CoE Resolutions with regard to the privacy of individuals *vis-à-vis* electronic databanks in the public and private sector[25] – distinguishes quality standards for personal data, on the one hand, and quality standards for the processing of personal data, on the other, as being fundamental standards. Both are divided into more detailed principles that will now be dealt with in line with the two fundamental legal standards presented by the CoE.[26] Derogations are allowed but only in accordance with Article 9 that, in its turn, is modelled on Article 8 of the European Convention on the protection of human rights and fundamental freedoms (hereafter: ECHR).

The standards laid down by the Data Protection Convention are the standards implemented by the Directive and by the other first pillar instruments.

The scope of EC Directive 95/46 is limited to all Community activities known as the first pillar of the EU. The Directive needed to be implemented in national legislation by the Member States but it did not provide a rule on implementing it in criminal matters. A limited number of Member States took that step on their own initiative. However, this is not enough to refer to the Directive as a comprehensive legal instrument in all areas of EU competence. Regulation 45/2001 has a scope which is limited to data processing by the Community's institutions. Directive 2002/58 particularises and complements Directive 95/46 and is also limited to activities within the scope of Community law. Thus, also these instruments are too limited in their scope to be comprehensive data protection instruments.

The newest instrument in data protection, the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereafter: the Framework Decision on data protection in criminal matters),[27] relies on the same basic standards stemming from the Data Protection Convention. Similar to the Data Protection Convention, the Framework Decision includes standards on personal data as such, as well as standards on the collection, use and dissemination of data and transborder data flows. In that sense it would be wise to refer to the Framework Decision on data protection as a comprehensive data protection instrument for the field of criminal matters. However, the instrument has a limited scope. It is firstly limited to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Secondly, it only includes the transfers of personal data that a Member State has received from another Member State. It does not include the processing of personal data that a Member State has gathered nationally.

It is thus clear that the EU has no comprehensive data protection scheme in place that covers all areas of EU competence. Even though the literature often refers to Directive 95/46 as

22 Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *OJ* L 238, 22.9.2000, pp. 19-62.

23 Convention of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (Prüm Convention), 10900/05, 7 July 2005.

24 Benelux Convention on cross-border police cooperation, 8 July 2004, <http://www.benelux.be>.

25 Resolution (73)22, 26.09.1973 and Resolution (74)29, 20.09.1974.

26 *ETS*, no. 108, Explanatory Report, Para.40.

27 Framework Decision 2008/977/JHA, *OJ* L 350, 30.12.2008, pp. 60-71.

a comprehensive legal instrument,[28] its scope is too limited to cover all areas of EU competence. The Framework Decision on data protection in criminal matters finally offered data protection legislation for the third pillar, but also this instrument is hindered by a limited scope due to the fact that it does not encompass domestic data processing. In any case, the data protection provisions in the applicable instruments should at least be consistent with each other.[29]

2.2.2. Data protection standards

A high level of protection cannot be ensured with inconsistent data protection provisions. Thus this statement implies that the currently applicable instruments, as well as the provisions they include, are consistent with each other. Therefore, the basic standards of data protection as laid down in the Data Protection Convention should be studied as well as their implementation by the EU in the legal instruments which are currently applicable. These basic standards are divided into quality standards of the personal data as such, quality standards of the processing of personal data and the adequacy requirement as the standard for the transfer of personal data to a third state or authority.

Article 5 of the Data Protection Convention – modelled on the basic standards for data protection presented by the aforementioned CoE Resolutions[30] – distinguishes quality standards for personal data, on the one hand, and quality standards for the processing of personal data, on the other, as being fundamental standards. Derogations are allowed, but only in accordance with Article 9 of the same Convention.

The protection of personal data as such encompasses the accuracy, adequacy and relevance of the personal data that are gathered. In addition, personal data should not be excessive in relation to the purpose for which they are gathered.

The Data Protection Convention and Directive 95/46 provided the Member States with two cumulative methods to ensure the accuracy of the gathered data. Firstly, the data controller should ensure that data are correct and updated.[31] Secondly, the Data Protection Convention, as well as the Directive, give the data subject the right to have the relevant data corrected or erased. This implies a notification to the data subject that data have been gathered and the purpose thereof, unless the individual already has this information or unless other exceptions apply such as the prevailing interests of an ongoing investigation.

As laid down by the Data Protection Convention[32] and the Directive[33] the provision on the quality of personal data as such includes a qualitative and a quantitative condition. The essence of the principle lies in the fact that no data should be collected and stored with a view to a potential future use, the purpose of which is uncertain.[34]

---

28 R.G. Boehmer & T.S. Palmer, 'The 1992 EC Data Protection Proposal: an Examination of its Implications for the US Business and the US Privacy Law', 1993 *American Business Law Journal* 31, p. 282; W.J. Long & M.P. Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise', 2002 *Journal of European Public Policy* 9, no. 3, p. 333 and A. Levin & M.J. Nicholson, 'Privacy law in the United States, the EU and Canada: the allure of the middle ground', 2005 *UOLTJ*, pp. 376-377.

29 *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July 2009, Para. 28.

30 Committee of Ministers, Resolution (73)22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 26 September 1973 and Committee of Ministers, Resolution (74)29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20 September 1974.

31 Art. 6(1)(d) and 6(2).

32 Art. 5(c).

33 Art. 6(1)(c).

34 This should be distinguished from the case in which data are gathered and kept for a particular foreseeable emergency which may never occur, for example, where an employer keeps details of the blood groups of its employees engaged in hazardous occupations. Information Commissioner, *Data Protection Act 1998, Legal Guidance*, 1998, p. 37.

The adequacy and relevance requirements aim at demonstrating the qualitative connection between the personal data and the purpose. If a direct link is non-existent – for example, the same result can be achieved by other means – the data cannot be adequate or relevant.

On the quantitative level, respecting the proportionality rule means that the data controller should, in each case, determine and distinguish the minimum amount of personal data needed in order to successfully accomplish their purpose and to limit its processing to these data.

Personal data should be obtained and processed fairly and lawfully. This rule was included so as to avoid the use of improper or illegitimate methods for data gathering,[35] which will be assessed by considering the interests of the data subject, the purpose as well as the nature of the processing.

Personal data should be stored for specified and legitimate purposes and should not be used in a way which is incompatible with those purposes. In Resolution 1973(22), the authorized use of data was still stricter as it was limited to the purposes for which the data had been collected, unless appropriate authorisation was obtained.[36] Similarly, Recommendation R(87)15 limited the use of personal data collected and stored by police authorities exclusively for police use.[37]

In order to define what can constitute a compatible purpose, it is first necessary to refer back to Article 8(2) ECHR. Every interference with the right to privacy should be legal and necessary in the interests of a legitimate aim in order to be allowed. This includes the gathering of personal data as well as the use that is made of this data.[38] Therefore, any use for a purpose other than the original purpose should equally be subject to these requirements. Additionally, the European Court of Human Rights (hereafter: ECtHR) has added three conditions, notably that violations of privacy should also be precise, foreseeable and proportionate.[39]

Even when personal data are adequate and relevant at the moment of their collection, it is possible that after a certain amount of time these data are no longer adequate and relevant in relation to the purpose for which they were gathered. For these reasons, the Data Protection Convention has specified that personal data can be saved in databases for as long as is required for the purpose for which they are preserved. After this period of time has passed, the data can still be retained but need to be separated from the name – the identifying factor – of the person they relate to.

When the gathering of the personal data and the use thereof is situated in two different states, an additional issue arises. In the case where both states are EU Member States, both are bound by the same rules and will therefore not find the personal data they exchange to be in jeopardy. However, in the case where personal data are transmitted from an EU Member State to a third state, personal data could possibly enter into a legal framework of data protection that offers fewer safeguards than the state of the data's origin.

It is not the Data Protection Convention itself, but the 2001 Additional Protocol[40] that provides a special requirement to protect personal data in this particular situation. The Member State transferring personal data to a third state is bound, first, to check the level of the data protection in the receiving state (or authority) on its adequacy. Thus, from an EU point of view

35 Res (73) 22, 26.9.1973, Explanatory Report, principle 3.
36 Res (73) 22, 26.9.1973, Explanatory Report, principle 5.
37 R (87) 15, 17.9.1987.
38 *Leander* v. *Sweden*, [1987] ECtHR, Para. 48 and *Rotaru* v. *Romania*, [2000] ECtHR, Para. 46.
39 European Data Protection Supervisor, *OJ* C 139, 23.6.2007, p. 5, Para. 20. *Malone* v. *United Kingdom*, [1984] ECtHR, Paras 67-68 and *Rotaru* v. *Romania*, [2000] ECtHR, Para. 55.
40 2001 Additional Protocol to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, *ETS*, no. 181.

the third state should have an adequate level of data protection. This requirement is included in Directive 95/46 and in the Framework Decision on data protection in criminal matters.

Nevertheless, the Additional Protocol to the Data Protection Convention has not been ratified by all Member States. Therefore, only those Member States which have ratified the Additional Protocol have genuine legislation on the transfer of all personal data – not only the data transmitted or made available by another Member State, but also those which the transmitting state gathered itself – to third states.

Additionally, no check-list on how to uniformly assess the adequacy of other states' data protection legislation is yet available. This diverse application of the adequacy requirement creates inconsistencies in the EU data protection scheme. In practice this could mean that a person involved in a criminal case on which both Member States A and B have gathered personal data sees his personal data being transferred from Member State A to a third state X without any adequacy check whatsoever, while his data held by Member State B are not transferred due to third state X not passing the strict adequacy assessment made by Member State B. Consequently, third state X could use the received data for purposes that are incompatible with the purposes for which the data were gathered as no adequacy assessment of its data protection provisions was made.

2.3. Consistency of the data protection provisions

The fourth paragraph in Chapter 2.3 of the communication introducing the Stockholm Programme starts with 'The current legal framework introduces a high level of protection'. It is necessary to note here that this statement was deleted in the draft Stockholm Programme. In fact, it was replaced by a more realistic point of view on the current situation as the European Council invites the Commission to 'evaluate the functioning of the various instruments which form the basis for the data protection regime in the EU (first pillar and third pillar)'.

In testing compliance with the data protection standards of the Data Protection Convention, the legal instruments enacted by the EU should be examined in as far as they encompass data protection provisions. The two instruments with the widest scope, although this is not a general scope, are Directive 95/46 and the Framework Decision on data protection in criminal matters. Both will be tested here as regards their compliance with the basic standards and thus their consistency with each other.

The first set of rules, which focused on compliance with the principle of the accuracy, adequacy and the relevance of the personal data in question, does not uncover dissimilarities. Both the Directive and the Framework Decision provide safeguards ensuring the accuracy and, where necessary, the completion or updating of the data.

Other instruments with a more limited scope – such as the aforementioned Europol Convention or the Schengen Implementation Convention – rely on a reference to the general principles of the Data Protection Convention or do not even mention these as all Member States have ratified the mother Convention and are thus bound by its provisions.

The second set of rules, aimed at the principles of purpose limitation and data retention, entails more derogation in the two legal instruments.

The wording of the purpose limitation principle in Directive 95/46 is very close to the wording used in the Data Protection Convention. Besides processing for the purpose for which the data were gathered, data can be processed for compatible purposes. The Directive stops there, but the Framework Decision does not. The latter includes derogations from the purpose limitation principle that amount to purpose deviation. The use of the phrase 'for any other purpose' means that personal data can be exchanged for any purpose with the prior consent of the transmitting

Member State or with the consent of the data subject. Firstly, this means that the link between the original purpose and the final purpose is severed. However, it should here be noted that the purpose for which the data will be used is not always known when gathering the data. Secondly, this means that the consent of the person involved can be substituted by the consent of the transferring state. The consent of the state does not in itself justify any derogation from the purpose limitation rule. The necessity requirement can then only be fulfilled by demonstrating the necessity for protecting the rights and freedoms of others or in the interests of protecting state security, public safety and the monetary interests of the state or the suppression of criminal offences. This is not specified in the Framework Decision, however. Therefore, the purpose limitation principle is not fully complied with in the Framework Decision on data protection in criminal matters.

Similar provisions are incorporated in legal instruments on judicial and law enforcement cooperation that also include data protection provisions.[41] Also here the conclusion is that the purpose limitation principle is not fully complied with in the legal instruments governing data exchange in criminal matters.

Violating the principle of purpose limitation is a development that is closely linked to violations of the data retention principle. Both rules stemming from Article 5 of the Data Protection Convention are interconnected as saving data for a period of time that is longer than is necessary for the data increases their availability. Data that are available can be used for other purposes. In accordance with the Framework Decision on data protection in criminal matters, national law shall provide appropriate time-limits for the erasure of data storage or for a periodic review of the need for storing the data.

The provision of Article 9(1) of the Framework Decision does not apply in cases where the data are required for current investigations, prosecutions of criminal offences or the enforcement of criminal penalties, which is a confirmation of the basic data retention rule.

Therefore, the Framework Decision that provides a legal framework for data protection in criminal matters lives up to the standard laid down by the Data Protection Convention regarding data retention. Because Directive 95/46 uses an almost identical formulation in Article 6(1)(e) as was laid down in the mother convention, both instruments are consistent with regard to data retention.

The adequacy requirement is provided in both Directive 95/46 and the Framework Decision on data protection in criminal matters. Both instruments allow derogations from this basic requirement, but are very different concerning the scope of these derogations. Directive 95/46 provides for detailed derogations which focus on the first pillar field of commercial matters including transfers that are necessary for the conclusion of contracts at the request or in the interest of the data subject.

The Framework Decision on data protection in criminal matters provides for derogations that are rather broad. In accordance with this instrument, four conditions need to be fulfilled in order to transfer personal data to third states or bodies and checking the adequacy of the level of the data protection of the receiving party is one of them. The other conditions are the necessity of the transfer for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the responsibility of the receiving authority for these tasks. Finally, the consent of the Member State that has transferred the data is a requirement. These conditions need to be fulfilled cumulatively. However, the derogations that are allowed

41 See in elaborate detail E. De Busser, *Data protection in EU-US criminal cooperation*, 2009, pp. 127-183.

undermine the concept of adequacy. If the transferring Member State's national law so provides because of the legitimate specific interests of the data subject or legitimate prevailing interests (especially important public interests) or when the receiving third state or body provides adequate safeguards, there can be a deviation from the adequacy requirement.

Specifically the interests of state security can – even when they are legitimate and prevailing – ensure that personal data gathered for criminal purposes are transferred in order to be processed for administrative purposes. And all this while skipping the requirement of an adequacy check, thus releasing the data into a legal system where data protection provisions are possibly not adequate in comparison to EU standards.

2.4. High level of data protection?

The communication introducing the Stockholm Programme includes the statement that 'the current legal framework introduces a high level of protection'.[42] But are the data protection standards truly that high in the basic EU legal instruments on data protection? The enthusiasm with which this statement was made should be moderated. And it was rightfully moderated in the draft Stockholm Programme published in October 2009. It is refreshing to see the European Council in this document inviting the Commission to evaluate the functioning of the instruments which form the basis for the data protection regime in the EU and present, where necessary, further legislative and non-legislative initiatives to maintain the effective application of principles such as the purpose, the proportionality and the legitimacy of processing, limits on storage time, security and confidentiality.

With regard to the purpose limitation principle, a call for an evaluation of the functioning of these instruments is a good thing. The data protection provisions in the applicable instruments on judicial and police cooperation in criminal matters show that the application of the purpose limitation principle moves in the direction of purpose deviation.[43] The use of widely formulated provisions allows the processing of data for other purposes that are not always compatible with the original. This is particularly visible in the new Framework Decision on data protection in criminal matters. The other legal instrument regarding data protection, Directive 95/46, remains close to the mother convention encompassing the data protection standards. Thus, inconsistencies exist between the two main data protection instruments in the EU with regard to the purpose limitation principle. This is not the case with regard to the data retention principle.

With regard to the transfer of personal data to third states, this is not mentioned in the chapter on the protection of personal data and privacy, but is briefly touched upon in the chapter on 'Europe in a global world – the external dimension of freedom, security and justice'. Nevertheless, when scrutinizing the application of the adequacy requirement we can only conclude that it is not entirely satisfactory. Not being a general requirement for all EU Member States to apply, it is also not laid down in a strict manner in the Framework Decision on data protection in criminal matters due to derogations that can encompass a range of situations in which no adequate level needs to be guaranteed. Especially in the sensitive field of criminal matters, this can potentially entail data protection violations when data are transferred to other criminal justice systems. Compared to the derogations provided by Directive 95/46, both instruments are not consistent with each other.

42 COM(2009) 263/4, p. 8.
43 See in elaborate detail E. De Busser, *Data protection in EU-US criminal cooperation*, 2009, pp. 127-183

3. The cooperation with the US on data protection could serve as an example

The communication of June 2009 introduced the statement 'the work on data protection conducted with the United States could serve as a basis for future agreements'.[44] This indicated that future bilateral and multilateral agreements should be based on the instruments which the EU, Europol and Eurojust have concluded with the US encompassing data protection provisions. Fortunately, this statement was deleted from the text that was published as the draft Stockholm Programme in October 2009. Nonetheless, it should be examined whether this statement was made with good reason. In other words, is it justified to state that the transatlantic cooperation regarding data protection can serve as an example for future agreements with third states?

The word 'example' is a strong term to use in this context. In order to use it correctly the basic standards of data protection applicable in the EU should have been complied with in the cooperation with the US on data protection. Whether this is the case should be studied by checking the application of the standards on personal data as such and the application of the standards on the processing of personal data. As a third element, the application of the adequacy requirement should be examined in transatlantic relations in criminal matters.

The application of these three standards should be studied in all agreements that have so far been concluded on cooperation in criminal matters between the EU and the US. This means that the two Europol-US Agreements and the Eurojust-US Agreement should be studied as well as the 2003 Agreement on mutual legal assistance between the EU and the US. The agreements on passenger name record data (further: PNR agreements) will be touched upon briefly as the scope of this article does not allow an in-depth examination of the agreements. Thus, I will only highlight the compliance of the EU with its data protection standards in these agreements.

3.1. Law enforcement cooperation in criminal matters

Europol concluded two agreements with the US, one in 2001 on non-personal data[45] and one in 2002 on the exchange of personal data and related information, the supplemental Europol-US Agreement (hereafter: 2002 Europol-US Agreement).[46] Logically, it is the latter that is relevant to this article. When examining this Agreement's data protection provisions, three main issues are striking.

First of all, Europol's own data protection rules[47] provide an adequacy requirement as a prerequisite for data transfers to a third state.[48] A four-step process should ensure a reasoned decision on the adequacy of the level of data protection that the receiving state or authority offers. However, this process has not been applied in the case of the supplemental Agreement between Europol and the US. The Agreement was concluded without evaluating the US level of data protection. Ignoring its own data protection provisions regarding the exchange of personal data with third states, Europol has rubber-stamped the American data protection system as adequate while no evidence has been produced to support this assessment.

---

44 COM(2009) 263/4, pp. 8-9.

45 Agreement between the United States of America and the European Police Office, 6 December 2001, European Council, 14581/01, 6-7 December 2001.

46 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, <http://www.europol.europa.eu>.

47 See also: P. De Hert & B. De Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in: B. Martenczuk & S. van Thiel (eds.), *Justice, Liberty, Security: New Challenges for EU External Relations*, 2008, (I.E.S. series no. 11), pp. 319-320.

48 Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third parties, *OJ* C 88, 30.3.1999, pp. 1-2.

Intensifying the impact of skipping this step, during the negotiations a phrase was included in the Agreement that banished all general restrictions on personal data exchange between the two parties. Logically, general restrictions include the adequacy requirement. The clarification adds that this should only be done in specific cases and when there is a real necessity.[49] What such a necessity may be has not been specified.

The explicit prohibition on general restrictions demonstrates the desire for a quick and smooth data exchange. Unfortunately, in this way the objective is accomplished by pushing aside a vital requirement safeguarding the EU's data protection standards in relations with third states.

Secondly, the 2002 Europol-US Agreement provides for rules that are closer to purpose deviation than purpose limitation. The transmission of information can be done in accordance with the Agreement for the purposes included in the request for data, which are 'deemed to include the prevention, detection, suppression, investigation and prosecution of any specific criminal offences and any specific analytical purposes' (Article 5(1)(a)). This phrase has a significant impact. Firstly, the US was unable to give Europol a list of authorities that would be eligible to receive data in accordance with this Agreement. Secondly, adding any specific analytical purpose to the possible purposes opens up the potential use of the data for intelligence-related purposes.[50] Not guaranteeing the necessity requirement, use for incompatible purposes is allowed by the 2002 Europol-US Agreement in a manner that does not comply with the EU data protection standards.

Thirdly, important parts on the scope of the cooperation agreement are included in the exchange of letters instead of the text of the agreement.[51] For example, the exchange of letters of November 2002 states that the first sentence of Article 5(1)(a) includes, *inter alia*, an exchange of information pertaining to immigration investigations and proceedings, and to those relating to *in rem* or *in personam* seizure or restraint and confiscation of assets that finance terrorism or form the instrumentalities or proceeds of crime, even where such seizure, restraint or confiscation is not based on a criminal conviction.[52] Europol's mandate does not stretch outside the scope of criminal offences that are not related to offences within its objective.[53] Thus, immigration investigations and proceedings should not be dealt with by Europol, which means that Europol is applying purpose deviation rather than purpose limitation and is thus transgressing the data protection standards.

The explanatory note to this Agreement specifies that widening the purposes to include administrative immigration[54] investigations and proceedings only applies to the US authorities.[55] The note does not include a similar statement on seizure, restraint and confiscation investigations and proceedings. Nevertheless, the problem is really the fact that the US authorities can ask for

49 13696/1/02, 28 November 2002, p. 10.
50 G. Vermeulen, 'Transatlantisch monsterverbond of verstandshuwelijk?', 2004 *Panopticon*, p. 97.
51 S. Peers, *The exchange of personal data between Europol and the USA*, Statewatch Analysis 2003, Para. 4, <http://www.statewatch.org>.
52 13996/02, 11 November 2002, p. 3. See also V. Mitsilegas, 'The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data', 2003 *EFAR* 2003 8, pp. 521-522.
53 JUSTICE briefing to the House of Lords Select Committee on the European Union, Sub-Committee F (Social Affairs, Education and Home Affairs) on a Supplemental Agreement between Europol and the United States of America on the exchange of personal data and related information, November 2002, Paras 5-6.
54 According to JUSTICE, the competence to exchange personal data relating to immigration falls within the scope of the rules relating to data protection within the first pillar including the European Parliament and Council, Regulation (EC) no. 45/2001, *OJ* L 8, 12.1.2001, p. 1. 'Europol is not a Community institution and as such is not governed by this Regulation. The exchange of personal data relating to immigration can in no way be considered to be a function of Europol.' *Ibid.*, Para. 7.
55 13696/1/02, 28 November 2002, p. 7.

information on proceedings *in rem*, where the EU only allows *in personam* confiscations and seizures.[56]

The tradition of sharing data within the multitude of agencies that the US harbours has significant consequences with regard to the purpose limitation rule. Especially – but not exclusively – since the terrorist attacks of 11 September 2001, legislative efforts have been made to break down the so-called 'wall' between the law enforcement and the intelligence community.[57] Legislation on the gathering and processing of personal data allows law enforcement authorities to use investigative techniques based upon the lower standards that used to be reserved for gathering intelligence.[58]

Nevertheless, it is the possible use of personal data for other – incompatible – purposes in the transatlantic cooperation in criminal matters that constitutes the true violation of the data protection standards. Even though a High-Level Contact Group,[59] consisting of senior officials from both the EU and the US, introduced a common definition of purpose limitation, the concept of purpose limitation is not identical in both criminal justice systems. On the contrary, 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'.[60] If the definition would be accompanied by a definition of the terms, more specifically, the term 'law enforcement' and by the practice of data sharing in the US, the title 'common principle' would thus be highly inappropriate.

Fourthly, the Agreement lacks a clear time-limit regarding the retention of personal data that corresponds with the standard laid down in the Data Protection Convention. The lack of a provision on data retention is problematic because the US legal framework does not contain a data retention principle. Data retention in a general standard format is unknown in the US. It is only applied in specific legislation.[61] Where the EU standard encompasses no storage of data after it is no longer necessary for the purpose for which they were stored, the US starts from a general storage rule with only specific and explicitly authorized erasures of data.

The fact that no general rule on data retention is applicable in the US makes this issue an even more complicated one to agree upon, not in the least because of its link – again – to the data sharing environment. Not knowing which authority receives the data from another authority means not knowing what the time-limits are for the specific receiving authority.

---

56 G. Vermeulen, 'Transatlantisch monsterverbond of verstandshuwelijk?', 2004 *Panopticon*, p. 98. See for example Art. 1(d) of the 1990 CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime; Council, Framework Decision 2003/577/JHA, 22 July 2003 on the execution in the European Union of orders freezing property or evidence, *OJ* L 196, 2.8.2003, pp. 45-55 and Framework Decision 2006/783/JHA, *OJ* L 328, 24.11.2006, p. 59. However, even in the case of proceedings *in rem* – proceedings not related to criminal offences – mutual assistance is not entirely excluded, this depends on the national legislative framework of the requested state. See further: G. Stessens, 'Belgian report AIDP Preparatory Colloquium on Corruption and Related Offences in International Business Transactions', 2003 *RIDP* 47, no. 1/2, p. 144 and M. Borgers, *International Cooperation in Confiscation Matters and Dutch Legislation: Points of Attention for Effective Cooperation in the European Union*, September 22, 2005, pp. 1-10, <http://ssrn.com/abstract=851064>.

57 See in elaborate detail: E. De Busser, *Data protection in EU-US criminal cooperation*, 2009, pp. 281-291.

58 For example, an application for a court order allowing electronic surveillance within the terms of the FISA needs only to have the obtaining of foreign intelligence information as a significant purpose, not as the only purpose. This means that in every investigation that has a connection with foreign intelligence, surveillance can be conducted without a traditional court order. 50 USC Para. 1804(7)(B). See also J.A.E. Vervaele, 'Gegevensuitwisseling en terrorismebestrijding in de VS en Nederland: emergency criminal law?', 2005 *Panopticon*, p. 33 and P.T. Jaeger *et al.*, 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act', 2003 *Government Information Quarterly*, no. 20, p. 299.

59 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, p. 2.

60 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, <http://www.edps.europa.eu and 9831/08>, 28 May 2008, p. 4.

61 For example, the retention of personal data on persons renting video tapes in the Video Privacy Act. 18 USC Para.2710(e).

3.2. Judicial cooperation in criminal matters

Even though the 2002 Europol-US Agreement was the first agreement in the transatlantic relations with an EU body to cover the exchange of personal data in criminal matters, two out of three data protection issues that can be seen in the 2002 Europol-US Agreement are also visible in the Eurojust-US Agreement.[62] The issue concerning the principle of data retention has been complied with in the Eurojust-US Agreement.

Similar to Europol, Eurojust is bound by the adequacy requirement.[63] Similar to Europol, no assessment of the adequacy of the American data protection level is provided and the 'no generic restrictions' clause is also included in the Eurojust-US Agreement.

Additionally, the widening of the purposes for which personal data can be processed after an exchange is equally supported in the Eurojust-US Agreement. Including the phrase 'for any other purpose' without compensation in the shape of a necessity requirement or the consent of the data subject does not correspond to the concept of purpose limitation as it was provided for by the Data Protection Convention.

The EU-US mutual legal assistance Agreement (hereafter: EU-US MLA Agreement)[64] was the first agreement to be concluded by the EU as a group of states and the US by means of a combination of Articles 24 and 38 TEU. The agreement's data protection provisions are clearly modelled on the provisions of the Eurojust-US Agreement. The provisions on purpose limitation are similarly structured and the adequacy requirement is equally pushed aside. Thus, transatlantic relations in criminal matters still continue along the same path when data protection is concerned.

3.3. PNR Agreements

The agreements concluded with regard to the exchange of passenger name record data[65] are a rather peculiar case in this respect since the successively concluded agreements are neither part of the cooperation between law enforcement authorities, nor between judicial authorities. The PNR Agreements were concluded between the EU and the US by combining Articles 24 and 38 of the Treaty on the European Union in order to exchange passenger name record data from European air carriers to the US Department of Homeland Security, more specifically Customs and Border Protection.[66] The first agreement was annulled by the Court of Justice[67] due to its first pillar legal basis, even though this required an adequacy assessment of the American data protection system. The adequacy check was then no longer a formal prerequisite using a third pillar legal basis. However, the EU did not comply with its own data protection standards when agreeing to an exchange of personal data with an administrative authority which can share the data with other authorities in the US for the purposes of criminal investigations. Furthermore, the introduction of the term 'dormant' data and the uncertainty regarding the time-limit for storing the PNR data due to data sharing by US authorities means that also the data retention principle

62 Agreement between Eurojust and the United States of America, 6 November 2006, <http://www.eurojust.europa.eu>.
63 Decision no. 2002/187/JHA, *OJ* L 63, 6.6.2002, pp. 1-13 and Council, *OJ* C 68, 19.3.2005, pp. 1-10.
64 Agreement of 25 June 2003 on mutual legal assistance between the European Union and the United States of America, *OJ* L181, 19.7.2003, pp. 34-42.
65 Agreement of 17 May 2004 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. *OJ* L 183, 20.5.2004, pp. 83-85 and the corrigendum at *OJ*.L 255, 30.9.2005, pp. 83-85; 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, *OJ*.L 298, 27.10.2006, pp. 29-31 and Agreement 23 July 2007 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), *OJ* L 204, 4.8.2007, p. 18.
66 For an elaborate overview, see E. De Busser, Data protection in EU-US criminal cooperation, 2009, pp. 358-384.
67 Case 317/04 and Case 318/04, *Parliament* v. *Council*, [2006].

was not fully complied with in these agreements. The data protection safeguards which the EU requested are not very apt to remedy this situation.[68]

3.4. Conclusions: No American meals for EU citizens

According to the communication introducing 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.'[69] The draft Stockholm Programme puts an end to this statement after the first sentence, although it is still a profound statement to make.

Studying the compliance of the EU with its own standards in its two main legal instruments on data protection, Directive 95/46 and the new Framework Decision on data protection in criminal matters, the conclusion is not very positive. Both instruments are not consistent with each other when data protection standards are concerned and the differences cannot be explained by their different scope. Additionally, the Framework Decision is not fully in line with the standards as laid down in the basic Data Protection Convention. Thus, the EU does not fully comply with its own standards when developing a legal framework for data processing in the third pillar. Both legal instruments can thus not provide a comprehensive legal framework for the EU, not only because of their scope but also because of their inconsistencies.

Should the EU-US cooperation in criminal matters serve as a role model for data protection? No. The agreements concluded in the transatlantic cooperation in criminal matters continue along the same line of a lack of compliance with the basic EU standards on data protection.

Without a solid check of possible inconsistencies between the EU level of data protection and the level of data protection by the US, personal data can now be transferred with American law enforcement and judicial authorities and be 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 Data Protection Convention – which has been ratified by 41 states – 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 – which has been ratified by 25 states – loses its meaning.

Even though not every third state will apply purpose deviation rather than purpose limitation and not every third state has a tradition of data sharing, encouraging the creation of Agreements based on the example of the PNR Agreements, 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.

Therefore, it should be stressed that it is a very positive development to omit the reference to the transatlantic cooperation as an example from the draft Stockholm Programme.

68 E. De Busser, *Data protection in EU-US criminal cooperation*, 2009, pp. 380-383.
69 COM(2009) 263/4, pp. 8-9.