Chapter 9
The Adequacy of an EU-US Partnership

Els De Busser

9.1 Transatlantic Hopes and Wishes

The EU and the US represent a total of almost 800 million people and have set up a considerable cooperation in criminal matters by exchanging personal data for the purpose of prevention, detection, investigation, or prosecution of criminal offences. This cooperation is characterized by bilateral agreements as well as by agreements between the EU (representing its Member States) and the US and agreements by the EU's bodies (responsible for judicial and law enforcement cooperation in criminal matters) and the US. This cooperation is also characterized by differences in legislation and attitude towards the protection of personal data, however, resulting in reports on illegal transfers of personal data[1] and the rejection of the Agreement between the EU and the US on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (the Interim Agreement).[2] These experiences have led to attempts to bring both parties to the table to negotiate a general agreement that can govern the transatlantic exchange of personal data for the purpose of prevention, detection, investigation, or prosecution of criminal offences. The following questions remain: Which course should the transatlantic exchange of personal data in criminal matters take? How can we make a compromise between the conditions the EU wants to see fulfilled and the wishes that the US authorities have or is a compromise simply impossible? Let us first look at what both sides would like to achieve with regard to transatlantic data exchange.

On the EU side, the European Commission recognized that the EU's legal framework on the protection of personal data is in need of review. In spite of the

[1] See, for example, Lichtblau and Risen (2006), and Modderkolk and Wester (2011).

[2] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, O.J. L 8, January 13, 2010, 11–16.

E. De Busser (✉)
Max Planck Institute for Foreign and International Criminal Law,
Günterstalstraße 73, 79100 Freiburg, Germany
e-mail: e.busser@mpicc.de

S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?,*
DOI 10.1007/978-94-007-2903-2_9,

technological advancements in data processing, the basic data protection principles are still considered valid, even though their application needs to be clarified.[3] However, the entry into force of the Lisbon Treaty and the dissolving of the three pillars require a new general instrument on data protection. In addition, the Commission has recognized that the 2008 Framework Decision on Data Protection in Criminal Matters[4] is not an adequate instrument.[5] Finally, even when the principles governing data protection still prevail amongst the plethora of new techniques and concepts, such as data mining, cloud computing, and behavioral advertising, the concrete rules on data gathering and processing need to be revised and updated in view of these new circumstances.

What the EU wants is, first of all, a revision of the current data protection legal framework. For this purpose, the Commission presented a comprehensive approach to data protection in the EU.[6] Since the exchange of data with third states, especially the US, has intensified significantly since 2001, the Commission's communication also includes a chapter on the global dimension of data protection. Under this heading, two main objectives are listed. Firstly, the procedure for allowing data transfers to third states should be simplified and clarified. Third states need to be checked as to whether their legal framework on data protection is adequate within the framework of EU rules before they can receive any personal data transmitted from a Member State. This adequacy procedure needs to be improved. Secondly, the Commission aims to promote universal principles of data protection. This means that cooperation with organizations such as the UN, the Council of Europe, and the Organization for Economic Cooperation and Development (OECD) should be strengthened as far as data protection is concerned. The Commission's approach was not presented with the transatlantic cooperation in criminal matters in mind. Nevertheless, one cannot discuss the EU-US negotiations on new data transfer agreements without considering the Commission's plans.

Besides the review of its own data protection framework, the EU has been active in negotiating agreements with the US involving the transfer of personal data for the purpose of prevention, detection, investigation, or prosecution of criminal offences. The idea of introducing a general agreement on data protection in transatlantic cooperation in criminal matters took shape and negotiations were taken up in December

---

[3] European Commission, Comparative study on different approaches to new privacy challenges, in particular in the light of new technological developments, Final Report, 21 (2010).

[4] Framework Decision of November 27, 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L 350, December 30, 2008, 60–71.

[5] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010)609 final, November 4, 2011, 13–15 (further: COM (2010) 609 final). See also European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—A comprehensive approach on personal data protection in the European Union, January 14, 2011, 26–28.

[6] COM (2010) 609 final.

2010. It is the intention of the European Commission to use this future agreement as an umbrella instrument, not only for future agreements with the US but also for application to the existing agreements.[7]

Thus, the objectives on the EU side are threefold a simple and clear procedure for allowing data transfers to third states, universally valid data protection principles, and for the existing and future transatlantic cooperation to be governed by standards equivalent to the European standards.

On the US side, the objectives are also clear: smooth delivery of personal data from the EU judicial and law enforcement authorities, EU air carriers (passenger name record data), and financial data controllers (the Society for Worldwide Interbank Financial Telecommunication or SWIFT). Existing agreements with the EU and with Europol and Eurojust do not hide the fact that there should not be too many restrictions on the transatlantic flow of data. Ultimately, it was the European Council that asked the Commission to prepare a recommendation for the "negotiation of a data protection and, where necessary, data sharing agreements for law enforcement purposes with the United States." According to the US, the existing agreements should nonetheless remain untouched. The planned retroactive application of the future umbrella instrument was thus not well received by the US delegation to the EU. For these reasons, we can state that the goals on the US side are transparent and straightforward, namely trouble-free data transfers.

Are the EU's and the US' aims for transatlantic cooperation in criminal matters compatible, and how should we go about forming them into an agreement? This is the central question I will attempt to answer in this contribution. In Sect. 9.2, the scope of this agreement is analyzed, including the meaning of the key concepts. Sect. 9.3 focuses on the prerequisite for personal data transfers from the EU to a third state, that is the decision—based on an assessment of the legal framework—that the requesting state has an adequate level of data protection. Such an assessment has not been made so far for the US. In addition, the procedure of assessing a state's level of data protection is under review. Therefore, it should first be clarified whether and how the adequacy procedure should be carried out. In this part of the contribution, the adequacy procedure is studied as to its theoretical framework and its practical implementation. The lack of consistency is highlighted followed by three significant remaining questions with regard to the adequacy procedure: which is the authority that should decide upon the adequate level of data protection of a state; what is the precise content of this assessment and when should this assessment take place?

In Sect. 9.4, the future of this adequacy procedure in the transatlantic cooperation is studied. The Commission is working on a new agreement with the US as to which adequacy requirement is applicable. At the same time, the Commission suggests having the US ratify the Council of Europe Convention for the Protection of

[7] Commission européenne, Proposition de recommandation du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union Européenne et les Etats Unis d'Amérique sur la protection des données personnelles lors de leur transfert et de leur traitement a des fins de prévention, d'investigation, de détection ou de poursuite d'actes criminels y compris le terrorisme, dans le cadre de la coopération policière et judiciaire en matière pénale, COM (2010) 252/2, Annex, May 12, 2010.

Individuals with regard to the Automatic Processing of Personal Data (further: Data Protection Convention)[8] and its Additional Protocol.[9] If this occurs, the adequacy procedure would no longer be needed in the transatlantic cooperation. To date, however, the US' data protection regime is based on other ideas than those of the Data Protection Convention.

It is important to note here that this contribution is written from the perspective of the EU and the EU legal framework and policy on data protection. The US legal framework and policy on data protection have only been included in the analysis when relevant for studying the transatlantic cooperation in criminal matters.[10]

9.2 Definition of Law Enforcement

It seems rather obvious when two parties are negotiating an agreement on exchanging information for the purpose of law enforcement that both have the same idea on what exactly law enforcement is. Nevertheless, it was—and still is—surprisingly difficult to define the term "law enforcement" or "law enforcement authority" in the context of transatlantic cooperation. In the 2006 Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities, a transparent definition of law enforcement is given for the EU Member States.[11] But the US has a complex landscape of state and federal authorities and of authorities involved in law enforcement and intelligence, often having double competences—such as the FBI and the CIA, which are both responsible for law enforcement and intelligence activities.[12]

The difficulties in joining the two approaches became clear during the negotiations on the 2002 Europol-US Supplemental Agreement.[13] Europol issued an informal explanatory note only representing Europol's opinion, in which the following statement was made: "From the start, the US side made it clear that it was impossible for them to indicate with any degree of accuracy, which authorities could be involved in using such information, given the fact that there are many different authorities, which would qualify as being involved in preventing, investigating and prosecuting criminal offences. This was especially true given the many different State and local authorities

[8] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS no. 108.

[9] 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 no. 181.

[10] For a more detailed analysis of the US legal framework and policy on data protection see De Busser (2009).

[11] Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities between the Member States of the EU, O.J. L 386, December 29, 2006, 91.

[12] See inter alia, Fijnaut (2004), Vervaele (2005), and Manget (2006).

[13] Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information, November 6, 2002.

responsible for such issues."[14] When talks on a general data exchange agreement with the US started, a High-Level Contact Group (HLCG) was established to prepare for this agreement inter alia by developing common definitions of data protection principles.[15] The HLCG, which included senior officials from the European Commission, the EU Presidency (supported by the Council Secretariat), and the US Departments of Justice, Homeland Security, and State, agreed on 12 common data protection principles, such as purpose specification/limitation and information security.

When defining the scope of the principles under consideration, the HLCG recognized that the EU and the US have different ways of describing "law enforcement purposes." In the EU, this covers the use of data for the prevention, detection, investigation, or prosecution of any criminal offense. In the US, this encompasses the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security as well as noncriminal judicial or administrative proceedings related directly to such offenses or violations. According to the HLCG, in practice, these different views on law enforcement may coincide to a large extent.[16]

To base a new agreement on the possibility that both parties may consider the scope of the agreement to correspond is not a secure basis.[17] The gap that inevitably occurs where two interpretations of scope do not coincide could lead to practical and legal difficulties in deciding whether a transfer of data is governed by the agreement or not. In fact, violations of data protection principles could be caused if data falling within this gap are transferred and considered to be transferred under the terms of the agreement by one party but not by the other. For example, the US would consider intelligence data to be exchanged for the purpose of national security, that is, for law enforcement purposes, but this transfer would not fall within the scope of the agreement from the EU's point of view. This means additional work is still needed to clearly define the scope of this future agreement on data transfers for law enforcement purposes.

9.3 Adequacy Procedure

Transferring personal data from an authority within the EU—including Europol or Eurojust as the EU's bodies for law enforcement and judicial cooperation in criminal matters—to an authority in a third state still means that the EU standards on data

---

[14] Council, 13696/1/02, 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, November 28, 2002, 11.

[15] Council, 9831/08, EU US Summit, June 12, 2008—Final Report by EU-US High-Level Contact Group on information sharing and privacy and personal data protection, May 28, 2008, 2.

[16] Ibid., 3–4.

[17] See also European Data Protection Supervisor, Press Release November 11, 2008, Opinion on transatlantic information sharing for law enforcement purposes: Progress is welcomed, but additional work is needed, 13.

protection need to be respected. This can take place either by making the transfer to a state that has ratified the Council of Europe's Data Protection Convention or by ensuring that the third state has an adequate level of data protection. Data transfers to a third state that is not a party to the Data Protection Convention is thus still possible if this state has a data protection regime that offers safeguards for the requested data that are appropriate from the EU's point of view. This does not mean that the data protection regime of the requesting state must be identical, but an assessment needs to take place as to whether it is adequate. It is not the Data Protection Convention but the above mentioned Additional Protocol that lays down the adequacy procedure in Article 2 on transborder flows of personal data to a recipient, which is not subject to the jurisdiction of a Party to the Convention.

Article 2 of the Additional Protocol allows for derogations from the adequacy requirement that should be interpreted restrictively. Similar to the derogations from the provisions on human rights in the European Convention for Human Rights and Fundamental Freedoms (ECHR), they should at least be laid down by (national) law and be necessary for the protection of legitimate prevailing interests. The explanatory report to the Additional Protocol also refers to the same interests, based on which the right to privacy and data quality principles can be lawfully derogated from. This means derogations from the adequacy procedure are allowed to protect an important public interest, the exercise or defense of a legal claim, or the extraction of data from a public register. Derogations can also be made for the specific interest of the person whose data are transferred for the fulfilment of a contract with this person or in his interest, to protect his vital interests or if he has given his informed consent.

In case an adequate level of data protection cannot be assured by the requesting third state, another possibility for exchange still exists if the receiving state provides sufficient safeguards that are deemed adequate by the providing state. The safeguards can be limited, however, to include only the relevant elements of data protection and are only applicable to a specific transfer of data.

9.3.1 Theory and Practice

The adequacy procedure and the assessment that is part of it are thus significant elements of data transfers to third states and aims to protect the data protection standards that the EU Member States ensure. Unfortunately, this is not the case for all data transfers, as the requirement of making an adequacy assessment is not a uniform requirement. It is not even a uniform requirement in the field of law enforcement and judicial cooperation in criminal matters, which is—due to the sensitive nature of the data—a field that would surely benefit from consistently protecting EU standards in matters of transfer to a third state. On the contrary, the Framework Decision on Data Protection in Criminal Matters includes the adequacy requirement but is only applicable to data that the providing Member State receives from another Member State. This means that data gathered by a Member State itself can be sent to a third state without having to check the third state's level of data protection. Obviously,

if the providing Member State has laid down the adequacy procedure in its own national law, it would still be obliged to check the requesting third state's level of data protection.[18]

The only type of data transfer for which an adequacy assessment should be made in every case concerns the transfer of data for activities falling within the scope of the former first pillar, that is, Community law. However, research has proven that for these transfers there is no consistency in compliance with the provisions of Directive 95/46/EC.[19]

In the field of law enforcement and judicial cooperation in criminal matters, Europol and Eurojust should not be overlooked. These two bodies each have binding adequacy procedures in their own respective data protection rules that are independent from the Framework Decision on Data Protection in Criminal Matters. The differences between the procedures that Europol[20] and Eurojust[21] have laid down for themselves are significant, and the mandatory nature of the adequacy assessment as a prerequisite for data transfers to third states is clear. Nonetheless, compliance with this procedure is also problematic here, especially as regards cooperation with the US.

Europol has declared that the US ensures an adequate level of data protection, but no complete assessment has been made. Still, personal data transfers are made under the terms of the 2002 Europol-US Supplemental Agreement. Eurojust has laid down in its agreement with the US that no general—"generic"—restrictions for processing of data with respect to the legal standards of the receiving party may be imposed as a condition for delivering information.[22] Obviously, this should be read as a denial of any adequacy procedure whatsoever, since the assessment that is part of the procedure is exactly that: it is a condition without which information should not be transmitted; it is a restriction with respect to the third state's legal standards on processing the received data, and it is a restriction of a generic nature. This means that it is not applicable to only a specific group of data but is binding for all personal data transfers falling within the scope of the agreement.

When considering the agreements the EU has made to represent its Member States, two cooperation agreements with the US are relevant: the 2003 EU-US Agreement

[18] A recent study ordered by the European Commission, revealed that the national laws of the member states do not fully comply with Article 26 of Directive 95/46/EC that provides in the adequacy assessment for transborder data flows. Inconsistencies lie in the explicit or implicit nature of legal provisions concerning adequacy, the authority deciding upon adequacy (Commission or member state authority) and divergences in the application of the special conditions under which data may be sent to third countries without adequate data protection. See for a full report: Korff (2010).

[19] Ibid., 91–94.

[20] Council of the European Union, Act March12, 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies, O.J. C 88, March 30, 1999, 1.

[21] Council Decision of February 28, 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, O.J. L 63, June 6, 2002, Article 27, § 4 and Council, Rules of procedure on the processing and protection of personal data at Eurojust, O.J. C 68, March 19, 2005, Article 28, §§ 2 and 3.

[22] Article 10, Agreement between Eurojust and the United States of America, November 6, 2006.

on Mutual Legal Assistance in Criminal Matters (2003 MLA Agreement)[23] and the 2010 EU-US Agreement on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (2010 TFTP Agreement).[24] The 2003 MLA Agreement included exactly the same provision prohibiting all generic restrictions in order to facilitate the data flow as was the case in the above-mentioned Eurojust-US Agreement.

The 2010 TFTP Agreement was not only unique before it was enacted, due to the historic rejection of the first text—the Interim Agreement—by the European Parliament in February 2010.[25] It also demonstrated another creative take on avoiding the adequacy procedure by laying down the following provision: "subject to ongoing compliance with the commitments on privacy and protection of personal data set out in this Agreement, the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for the purposes of this Agreement."[26] This provision was identical in the Interim Agreement and in the adopted 2010 Agreement. The Agreement was thus based on the assumption of an adequate level of data protection rather than on a genuine assessment. Needless to say, the Article 29 Working Party—the independent EU Advisory Body on Data Protection and Privacy—did not like this provision. In fact, when the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs asked the Article 29 Working Party and the Working Party on Police and Justice—a specific working group of the Conference of Data Protection Authorities—to evaluate the Interim Agreement, the chairmen of both Working Parties expressed their concerns in a letter to the Committee. Their statement is clearly one of dissatisfaction: "Furthermore, the wording of Article 6 of the Interim Agreement, according to which the 'U.S. Treasury Department is deemed to ensure an adequate level of data protection', has brought about a certain degree of perplexity amongst the Working Parties' members."[27] Both chairmen stress the fact that no independent assessment of the level of data protection by the US Department of the Treasury (UST) was made before concluding the Agreement and wonder whether the joint review that should be conducted by the parties (at the latest 6 months after entry into force) could take the form of an adequacy check. This could be the case; however, it would still not replace an assessment made before deciding upon an agreement, as it would be post factum and many data have been transferred already under the terms of a legal instrument that

[23] Agreement June 25, 2003 on mutual legal assistance between the European Union and the United States of America, O.J. L 181, July 19, 2003, 34–42.

[24] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, O.J. L 195, July 27, 2010, 5–14.

[25] See European Parliament Recommendation, A7–0013/2010, February 5, 2010 and Press Release, SWIFT: European Parliament votes down agreement with the US, February 11, 2010.

[26] Article 6, 2010 TFTP Agreement.

[27] Article 29 Data Protection Working Party and Working Party on Police and Justice, Letter to Juan Fernando López Aguilar, Chairman of the Committee on Civil Liberties, Justice, and Home Affairs, January 22, 2010.

may be considered to be inappropriate when it comes to the level of data protection of the UST. Furthermore, the first joint review of the 2010 TFTP Agreement that has been carried out on 17 and 18 February 2011 clearly states that it is a valuable tool for the assessment of the level of implementation of the Agreement and the UST's compliance with the safeguards included therein. This does not include the assessment of the adequacy of the UST's level of data protection.[28]

It would be unrealistic to state that consistency would be ensured if all Member States ratified the Additional Protocol to the Data Protection Convention,[29] since this neither guarantees practical compliance nor does it guarantee proper assessments that are not guided by political or economic objectives. Still, ratification by all Member States would be a first step towards introducing some uniformity into the adequacy procedure. The second step should be made by the Commission, which promised to clarify and simplify the establishment of an adequacy assessment.[30]

Establishing an assessment as to whether a data protection legal framework is adequate or not is a procedure that has raised many questions, which the European Commission is determined to solve. The most important questions relate to the authority that makes the adequacy assessment on the one hand and the content of such assessment on the other. Raab and Bennett already discussed five interrelated concerns also identified by other scholars at the time Directive 95/46/EC was adopted.[31] These concerns will form the basis of the following analysis, which will focus more on judicial and law enforcement cooperation in criminal matters than on Directive 95/46/EC.

9.3.2 Equal Rules

The first main concern is the emergence of "data havens" or "data shopping," which is a potential consequence of having different rules on data protection in different Member States. It cannot be prevented that Member States exchange personal data amongst themselves in accordance with the legislation on information exchange in criminal matters. This can result in third states relying on the Member State that seems to be the "easiest" to deal with in order to obtain the data they want. A Member State that has not ratified the Additional Protocol to the Data Protection Convention and is also not bound by an adequacy procedure in another way, for

[28] Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, March 16, 2011, 15.

[29] The protocol entered into force for Austria, Bulgaria, Cyprus, Czech Republic, Estonia, Ireland, Germany, Hungary, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Spain, Slovakia, and Sweden.

[30] COM (2010) 609 final, 15–16.

[31] Bennet and Raab (1997).

example, by national law, would be an easy target.[32]A similar situation could occur when a Member State that is bound by an adequacy procedure and has issued a positive adequacy assessment for a particular third state transfers personal data to this third state from other Member States or from a database set up among the Member States. Transmitting personal data received from other Member States for the purpose of prevention, detection, investigation, and prosecution of criminal offences corresponds to the scope of the Framework Decision on Data Protection in Criminal Matters. Article 13 of this Framework Decision makes the Member States—and not the Commission—responsible for making adequacy assessments of third states. Therefore, the situation described above is not unimaginable in the case of personal data related to a criminal case.

A solution would be to ensure uniform rules in all Member States. If all Member States would ratify the Additional Protocol to the Data Protection Convention, the adequacy procedure would at least be mandatory for all. Nevertheless, this does not ensure its equal application, that is, equal adequacy assessments, by the national authorities regarding the same requesting third state. As mentioned above, putting Member State authorities in charge of adequacy assessments for data exchange in criminal matters entails the risk of data shopping.

9.3.3 Which Authority?

The question of which authority makes the assessment has not yet been answered, because EU legal instruments on data protection allow adequacy assessments made by the Member States as well as by the European Commission. Directive 95/46/EC mentions both options, while the Framework Decision on Data Protection in Criminal Matters only mentions the Member States. Both options have advantages and disadvantages. The advantage of the Commission making the assessment is that one uniform decision on a third states' level of data protection is introduced on which all Member States can rely. The risk, however, is that evaluations made by the Commission are directed by wider political and economic concerns in relation to the third state concerned.[33] Furthermore, this may not just be a concern in the case of Commission assessments, as the EU-US agreements negotiated by the EU Member States—represented by the EU presidency—also skipped a full evaluation of the US level of data protection (cf. supra).

The main drawback of Member State assessments is that different conclusions in different states can create confusion. Due to the lack of uniform rules on how the evaluations are performed, Member States can apply diverging methods or include different elements of data protection legislation. For example, one Member State may also include the practical application of data protection legislation in the assessment, while another may only rely on "law in the books." The concern regarding divergent

[32] See also Korff (2010).

[33] Bennet and Raab (1997).

implementation laws in the Member States has been confirmed by the European Commission in its first report on the implementation of Directive 95/46/EC that provides for the adequacy requirement in its Articles 25 and 26.[34] This concern was recently also confirmed by a study of the national legislations.[35]

Furthermore, national authorities making the adequacy assessment tend to evaluate a third states' data protection regime from the point of view of their own legislation. Even when the national laws are implementations of EU legal instruments on data protection, they still differ considerably.[36]

There are significant advantages to introducing Article 29 Working Party (hereinafter 29 WP) as the central authority deciding upon the adequacy of the level of data protection in third states for all Member States. Firstly, the above-mentioned disadvantages, which are generated by a Member State's authority or the Commission making the assessment, are in principle avoided. The 29 WP consists of representatives of the data protection authorities of the 27 Member States, a representative of the European Data Protection Supervisor, and a representative of the Commission. In accordance with Directive 95/46/EC, the 29 WP members act independently and decide by majority voting. Thus, one could expect there to be fewer chances of economic or political interests prevailing over data protection interests. Obviously, chances of this happening can never fully be excluded. Secondly, the 29 WP as the central authority helps avert the fact that national data protection legislations differ, which causes national assessments of a third state's adequacy level to differ. Thirdly, it is already the task of the 29 WP to advise the Commission on the adequate level of data protection in third states.[37]Making these evaluations binding decisions for all Member States would thus not require a change in its working procedure, although it would naturally increase the workload of the members. In addition, this new competence would require an amendment to Directive 95/46/EC. In view of the disappearance of the former three pillars and the current review of the legal framework on data protection, it would be appropriate to amend the tasks of the 29 WP and widen its function to also include criminal matters.

It is not necessary to set up a new authority. Utilizing the expertise and working procedure of the 29 WP would promote clarity regarding the deciding authority as well as uniformity regarding data transfers from Member States to third states.

---

[34] European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265, May 15, 2003, 18–19.

[35] European Commission, Comparative study on different approaches to new privacy challenges, in particular in the light of new technological developments, Final Report, 2010, 92–93.

[36] Bennet and Raab (1997).

[37] See in the same sense: Working Party on the Protection of Individuals with regard to the Processing of Personal Data, XV D/5020/97-EN final, WP 4, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy, Discussion Document adopted by the Working Party on June 26, 1997, 3.

9.3.4 Content of Adequacy

The type of data transfer determines the content of the adequacy assessment. This is implied by the Explanatory Report to the Additional Protocol to the Data Protection Convention, which states that the provisions of Chapter II (basic principles of data protection) of the Convention should be taken into account when assessing the adequacy of the third state's legal framework. Nonetheless, this clarification is only valid as far as these principles are relevant for the specific case of transfer. Thus, the basic principles of data protection do not necessarily have to be taken into account for every data transfer.

The 29 WP already examined the content of an adequacy assessment in 1997 and published a discussion document on the central question of adequacy in the context of Directive 95/46/EC.[38] Even though it is not applicable to the field of criminal matters, the document provides solid guidelines on what an adequacy assessment should include. In this discussion document, the 29 WP identified three types of data transfers within the scope of Directive 95/46/EC: a transfer between an EU-based data controller and a data controller based in a third state; a transfer between an EU-based data controller and a data processor based in a third state who processes the data on behalf of the data controller, and a transfer between an EU-based data subject and a data controller based in a third state. In the field of information exchange in criminal matters, the first type of transfer is the most common one, as these exchanges are organized between law enforcement and prosecution authorities of different states. This means that the data are transferred from an authority that determines the purpose and means of processing the data to an authority that also has that competence, yet within the framework of different data protection legislation.[39]

Besides the 29 WP, the Europol Decision has incorporated a list of items to consider when evaluating a third state's level of data protection.[40] Unlike the 29 WP, Article 23 of the Europol Decision focuses on data exchange in criminal matters rather than on data exchange in commercial matters—which is focused on by Directive 95/46/EC—and includes elements of data processing rather than the principles governing data processing. The list contains: the nature of the data, the purpose for which the data is intended, the duration of the intended processing, the general or specific data protection provisions applying to the requesting authority, and whether or not the entity has agreed to specific conditions required by Europol concerning the data.

---

[38] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, XV D/5020/97-EN final, WP 4, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy, Discussion Document adopted by the Working Party on June 26, 1997.

[39] Ibid., 9.

[40] Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL), O.J. L 121, May 15, 2009, 49.

The 29 WP defined a list of content principles to consider when assessing adequacy and heads off this list with the purpose limitation principle.[41] The Europol list also starts with the purpose for which the data is intended. When exchanging personal data for the purpose of prevention, detection, investigation, or prosecution of criminal offences, one main concern is data regarding a person to whom the presumption of innocence (Article 6 ECHR) still applies. It is thus highly important that these data are only processed for this specific purpose or a purpose that is compatible therewith. For this reason, the purpose limitation principle should be a minimum requirement to be fulfilled when deciding upon the adequacy of a third state's data protection framework. Careless handling of the data and improper safeguarding of the proportionality principle can have crucial repercussions for an individual involved in a criminal investigation either as suspect, witness, or victim. Measures protecting the quality of the data and their proportionality in relation to the purposes for which they are processed, should therefore also be laid down in the legal framework of the third state concerned. The onward transfer of data to other third states should be restricted in the case of criminal matters. In investigations or prosecutions of criminal offences that have links to several states, however, an onward transfer could become necessary. Nevertheless, an adequate level of data protection should also be provided by the receiving third state. Finally, technical and organizational security measures should be in place in order to prevent tampering or loss of data. These measures may not be laid down in national law, yet the data controller in the third state should provide for a level of data security that is sufficient and appropriate for the risks that the processing of data presents.

Two other principles were identified by the 29 WP in the aforementioned discussion document: the transparency principle and rights of access, rectification and opposition. In information exchanges for the purpose of prevention, detection, investigation, or prosecution, these principles cannot be guaranteed in every case—in the interest of the criminal investigation. For this reason, they cannot be part of the minimum data protection rules included in an adequacy assessment.

In addition to content principles, enforcement and supervision mechanisms should be installed in a third state in order to provide for adequate protection of data transferred from an EU authority. The 29 WP rightfully stated that it is more efficient to define the objectives to be achieved by these mechanisms rather than requiring their mere presence.[42] This means that the assessment of a state's data protection system should go beyond the "law in the books" and evaluate whether the system provides for support to data subjects and appropriate redress as well as a substantial level of compliance with the data protection rules. The independence of the authorities involved is a prerequisite.

---

[41] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, XV D/5020/97-EN final, WP 4, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy, Discussion Document adopted by the Working Party on June 26, 1997, 6.

[42] Ibid., 7.

9.3.5 When to Assess or Reassess?

An additional question, especially if the 29 WP is to be introduced as the authority deciding upon the adequacy of third states' legislation, is the moment at which the assessment should be made. Since fast information exchange is of utmost importance in most international criminal investigations, the duration of an adequacy procedure should be considered.

A case-by-case approach as foreseen in Directive 95/46/EC can be quick but is unrealistic due to the high amount of data transfers, particularly in the case of criminal matters. Nonetheless, in the case of criminal investigations, an urgency procedure could be introduced by which a decision on the adequate level of data protection is made for one specific data transfer.

The 29 WP itself put forward the idea of white lists of third states with an adequate level of data protection. Even partial listing of a particular type of data transfers is suggested by the 29 WP.[43] An a priori list consisting of all third states with which Member States could safely exchange personal data would take the 29 WP a long time to compile, principally blocking data transfers in the meantime. However, it still seems to be the best option. The list would have to be reviewed regularly in order to keep up with amendments to legislation in the third states. Obliging third states to inform the 29 WP whenever data protection legislation is modified would be another option.

9.4 Future of Adequacy: Negotiating a New EU-US Agreement

The planned review of EU legislation on data protection happens to be in progress at the same time as negotiations for a general data protection agreement between the EU and the US. The background of this development is the transatlantic cooperation that has been intensified since the terrorist attacks of 2001 in the US. The European Council asked the Commission to propose a general agreement with the US on data protection and, where necessary, on data sharing for law enforcement purposes (future EU-US Agreement on data protection).

One of the main questions to be answered in this respect is whether the principles laid down in such an agreement would apply not only to future agreements covering data exchange but also to existing ones. The negotiating directives include the statement that the future agreement shall also apply to "*existing EU or Member States personal data transfer and processing agreements with the US for the purpose of preventing, investigating, detecting or prosecuting, criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal*

[43] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, XV D/5020/97-EN final, WP 4, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy, Discussion Document adopted by the Working Party on June 26, 1997, 3–4.

matters after a transitional period of three years."[44] The effect that this statement could have is considerable, especially with regard to the adequacy procedure.

Even when the focus is not on the bilateral agreements but just on the data transfers between the EU and the US, the future agreement would change the terms of four existing agreements mentioned above. They not only include the 2003 MLA Agreement and the 2010 TFTP Agreement, but also the 2002 Europol-US Supplemental Agreement and the 2006 Eurojust-US Agreement, as the latter two equally provide for personal data transfers in the framework of police and judicial cooperation in criminal matters. As explained in the previous section, it is precisely in preparing these four agreements that the EU, Europol, and Eurojust have not complied with the requirement of evaluating the US level of data protection.[45] Due to adequacy requirements laid down in the Framework Decision on Data Protection in Criminal Matters, the future EU-US Agreement on data protection should not be concluded without making an adequacy assessment.

Considering the bad experience that the European Parliament had with the 2010 TFTP Agreement that was recently reviewed and revealed the existence of oral instructions from the UST to Europol concerning the data transfers,[46] it can be expected that the parliamentarians will push strongly for a genuine evaluation of the US data protection system.[47]

If a genuine assessment of the US level of data protection were made, it would have significant effects on the content of existing legal instruments. Regarding the Europol-US Supplemental Agreement and the EU-US TFTP Agreement, this would mean that the assumption of an adequate level of data protection would finally be backed up by an assessment of the US data protection framework, followed by a decision on its adequacy regarding data transfers with the EU. With regard to the EU-US MLA Agreement and the Eurojust-US Agreement, it would follow that the prohibition of generic restrictions should be amended or deleted. Nevertheless, on October 26, 2010, the Ambassador of the US Mission to the EU, William E. Kennard, declared during a hearing on the future EU-US Agreement on data protection in the European Parliament that the US does not wish to renegotiate the existing agreements.

The negotiating directives themselves could be the answer to this problem, as the Commission considers it a desirable step for the US to ratify the Council of Europe

---

[44] Commission européenne, Proposition de recommandation du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union Européenne et les Etats Unis d'Amérique sur la protection des données personnelles lors de leur transfert et de leur traitement a des fins de prévention, d'investigation, de détection ou de poursuite d'actes criminels y compris le terrorisme, dans le cadre de la coopération policière et judiciaire en matière pénale, COM (2010) 252/2, Annex, Negotiating Directives, § 4, May 12, 2010.

[45] See also De Busser (2010).

[46] See the report by the Europol Joint Supervisory Body, Europol Inspection Report 11-07, Report on the Inspection of Europol's Implementation of the TFTP Agreement, conducted in November 2010 by the Europol Joint Supervisory Body, accessed on April 1, 2011.

[47] European Parliament, "SWIFT implementation report: MEPs raise serious data protection concerns," Press Release, March 14, 2011.

Data Protection Convention and its Additional Protocol.[48] As mentioned above, the Data Protection Convention lays down the basic principles of data protection that have been implemented in the EU, and its Additional Protocol is the general legal basis for the adequacy procedure. Thus, if the US would agree to accede to these two legal instruments, there would be no need for the entire discussion surrounding the adequacy procedure, as the US would have to implement the same data protection principles in its system. This idea is neither desirable nor realistic.

The US accession to the Data Protection Convention and its Additional Protocol is not desirable due to the significant differences between the US system of data protection and that of the EU. These differences already led to the creation of the Safe Harbor principles,[49] the so-called "undertakings" attached to the Commission's adequacy assessment concerning the transfer of passenger name records[50] and the rejection of the first TFTP Agreement in February 2010.[51] Research has proven that data protection legislation in the US and the EU is divergent rather than similar.[52]

The US accession to both legal instruments is unrealistic for two reasons. Firstly, it is questionable whether it is a realistic option to ask a state with a legal history that has—in comparison to the elaborate EU rules—not been characterized by detailed data protection rules to change its attitude as well as its legislation and adhere to a set of formerly unknown principles that would have to be implemented in national law. Secondly, the (recent) history of EU-US cooperation in criminal matters has demonstrated that it is also not reasonable to expect the US to embrace our umbrella data protection system. As explained above, the prohibition of generic restrictions indicates that a smooth and trouble-free data exchange should be the goal and not a complete transformation of the US data protection regime.

---

[48] Commission européenne, Proposition de recommandation du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union Européenne et les Etats Unis d'Amérique sur la protection des données personnelles lors de leur transfert et de leur traitement a des fins de prévention, d'investigation, de détection ou de poursuite d'actes criminels y compris le terrorisme, dans le cadre de la coopération policière et judiciaire en matière pénale, COM(2010) 252/2, Annex, Negotiating Directives, § 17, May 12, 2010.

[49] Commission Decision of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. L 215, August 25, 2000, 7–47.

[50] Commission Decision of May 14, 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 235, July 6, 2004, 11–14; Annex Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), O.J. L 235, July 6, 2004, 15–22.

[51] European Parliament Recommendation, A7-0013/2010, February 5, 2010 and Press Release, SWIFT: European Parliament votes down agreement with the US, February 11, 2010.

[52] De Busser (2009).

9.5 Conclusion

Returning to the hopes and wishes of both the EU and the US, the following remarks can be made. The listed goals that the EU set out for itself are exactly the goals for the future. All three of these goals are part of an approach that has not been realized yet while the US' desire of an effortless data transfer seems to be in full progress.

The objectives on the EU side were to have a simple and clear procedure for allowing data transfers to third states, universally valid data protection principles, and for the existing and future transatlantic cooperation to be governed by standards equivalent to the European standards. However, simplifying the adequacy procedure is an exercise that is more complicated than it looks at first sight. Only a portion of the questions that it raises have been touched upon in this contribution. Introducing the 29 WP as the central authority deciding upon the adequacy of third states' level of data protection is in principle a good idea and solves several of the questions mentioned above. Nevertheless, it should be stressed that the 29 WP is not yet equipped for this challenging task.

The adequacy procedure remains to be a thorny issue in the transatlantic cooperation in criminal matters. By drafting the future agreement on data protection both parties could attempt to solve this, however, due to the differences between the data protection framework of the EU and the US, additional safeguards will always have to be guaranteed as was done in the past.

Universally valid data protection principles and the equivalence of the data protection standards in the EU-US cooperation to the EU standards are both objectives that are unrealistic. The transatlantic cooperation in criminal matters in the past decade is a good example thereof. As agreements that have been concluded to exchange personal data for the purpose of prevention, detection, investigation, or prosecution of criminal offences in the transatlantic cooperation have all been drafted in order to facilitate the flow of personal data rather than to safeguard EU data protection standards, the US seems to have realized more of its hopes and wishes than the EU.

Especially when considering the recent inspection by the Europol Joint Supervisory Board of the implementation of the 2010 TFTP Agreement by Europol, including the lack of time for Europol to prepare for its new role and the receiving of oral instructions by the UST regarding the data transfers, it seems that the transatlantic flow is dictated more by the US' wishes than by the EU's.

References

Bennet, Colin J., and Charles D. Raab 1997. The adequacy of privacy: The European Union data protection directive and the North American response. *The Information Society* 13:245–263.

De Busser, Els. 2009. *Data protection in EU-US criminal cooperation.* Antwerp-Apeldoorn: Maklu.

De Busser, Els. 2010. Transatlantic adequacy and a certain degree of perplexity. *Eucrim* 1:30–36.

Fijnaut, Cyrille. 2004. Inlichtingendiensten in Europa en Amerika: de heroriëntatie sinds de val van de Muur en 11 September 2001. *Justitiële Verkenningen* 3:10–42.

Korff, Douwe. 2010. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Working Paper no. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, *European Commission DG Justice, Freedom and Security Report*.

Lichtblau, Eric, and Risen James. 2006. Bank data is sifted by U.S. in secret to block terror. *The New York Times,* 23. June.

Manget, Fred F. 2006. Intelligence and the criminal law system. *Stan. L. & Pol'y Rev.* 17:415–435.

Modderkolk, Huib, and Wester Jeroen. 2011. Via Zoeterwoude kon CIA 'iedere' euro zien. *NRC Handelsblad,* March 19–20:3.

Vervaele, John A. E. 2005. Gegevensuitwisseling en terrorismebestrijding in de VS en Nederland: Emergency criminal law? *Panopticon* 2005:27–52.