# Transatlantic Adequacy and a Certain Degree of Perplexity

Els De Busser

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

AUTHOR

Els De Busser

Assistant Professor
Universiteit Leiden

CITATION SUGGESTION

E. De Busser, "Transatlantic Adequacy and a Certain Degree of Perplexity", 2010, Vol. 5(1), eucrim, pp30–36. DOI: https://doi.org/10.30709/eu-crim-2010-01

Published in
2010, Vol. 5(1) eucrim pp 30 – 36
ISSN: 1862-6947
https://eucrim.eu

CC BY ND

The very least that one can say or write about the cooperation in criminal matters between the EU and the US is that it has intensified since 2001. The EU and its bodies that deal with criminal matters – Eurojust and Europol – have concluded agreements with US authorities. However, the data protection provisions in several of these agreements have raised eyebrows. The exchange of personal data is a crucial tool in judicial and law enforcement cooperation in criminal matters. The EU as an entity, but also Eurojust and Europol, entered into negotiations with the US in order to regulate the exchange of personal data that were deemed necessary for the purpose of prevention, investigation, and prosecution of criminal offences. A key requirement for the transfer of personal data from within the EU to a non-EU state (a third state) is the evaluation of whether this third state endorses a level of data protection that is adequate in comparison to the EU rules on data protection. This adequacy assessment should ensure the protection of personal data transferred to another legal system that applies different data protection rules.

When the US and the Council of the EU signed – on 30 November 2009 – a new Interim Agreement on the processing and transfer of financial messaging data for the purposes of the Terrorist Finance Tracking Program (TFTP), the European Parliament's Committee on Civil Liberties, Justice and Home Affairs examined the Agreement in order to recommend approval of the Agreement to the Parliament. The Committee asked the Article 29 Working Party (the independent EU Advisory Body on Data Protection and Privacy) and the Working Party on Police and Justice (a specific working group of the Conference of Data Protection Authorities) to evaluate this Interim Agreement. When dealing with the question of whether the US endorses an adequate level of data protection, a prerequisite for the EU for the exchange of personal data with the US, the following statement was made by the chairmen of both working parties: "*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*." Thus far, a thorough examination has not been carried out in order to conclude on the adequacy of the US data protection system. The observation made by the two Working Parties regarding the lack of a genuine assessment of the American data protection rules is, in fact, not an isolated case. No assessment was made before signing the Interim Agreement and no assessment had been made prior to the conclusion of other agreements in the past.

In this article, examples of cooperation agreements with the US are examined, where, undoubtedly, members of data protection authorities and other data protection experts have experienced a similar "degree of perplexity" due to the lack of an adequacy assessment.

First, the requirement for an adequate level of data protection will be clarified, followed by the challenges in applying this requirement. Subsequently, the agreements between the EU, Europol, and Eurojust, on the one hand, and the US, on the other, will be scrutinised with regard to their compliance with the adequacy requirement.

# Umbrella Legislation

The EU is known for utilizing "umbrella legislation" on the protection of personal data. This term refers to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Protection Convention)[1] as the comprehensive legal instrument that covers all types of automatically processed personal data regardless of the purpose for which they are processed. It is referred to as "umbrella legislation" due to this wide scope. Because all EU Member States have ratified the Data Protection Convention, the data protection principles laid down therein are also the principles governing the EU's legislation on data protection.

Therefore, when personal data are exchanged between authorities within one Member State or between authorities located in different Member States, they are transferred to a legal system that is bound by the same basic principles on data protection as the legal system they originated from. Obstacles caused by a difference in data protection rules will hardly occur in such cases.

Alternately, in a situation where the personal data are located in an EU Member State and transferred to a non-EU state (a third state), there are two possibilities. On the one hand, the receiving state could be bound by the Data Protection Convention[2] and thus by the same basic principles governing the EU's data protection regime. On the other hand, the receiving state could be a state that has a different view on data protection. This would mean that personal data could enter a legal framework that offers lower data protection safeguards than the EU Member State from which the data originated. The opposite case – stricter data protection rules in the receiving state – is equally possible, but would not give rise to many difficulties unless the smooth international exchange of data is hindered by applying stricter rules.

In order to protect the personal data transferred from a state bound by the Data Protection Convention to a state that is not bound by it, the Convention itself did not lay down any rules. However, one requirement was introduced[3] in the 2001 Additional Protocol to this Convention.[4] The Protocol obliges the states bound by it to assess the level of data protection of the receiving state. If the level of data protection endorsed by the receiving state is adequate, the transferring state can send the requested data. This is called the adequacy requirement.

The Additional Protocol is not the only instrument that lays down the adequacy requirement,[5] but it is the only one with an all-embracing – umbrella – scope including all personal data that are automatically processed. The adequacy requirement has also been copied in legal instruments that cover a more specific part of personal data processing.[6] This underlines the fact that the requirement of an adequate level of data protection has become known as a basic prerequisite for cross-border flows of personal data.[7]

# The Paradox of the Adequacy Requirement

As appealing as it may sound in theory, the adequacy requirement causes many questions to arise regarding the assessment of the level of data protection and regarding whether the Member State is bound by the requirement or not. It is a prerequisite that has been laid down with the purpose of guaranteeing the EU's level of data protection and having the objective of ensuring that personal data of EU citizens are not subject to misuse in third states. A prerequisite of such a significant objective should at least be clear in its meaning, and it should be made a uniform requirement for all transfers of personal data to third states. However, this is not the case. Especially with regard to the sensitive area of criminal investigations and prosecutions, it would be logical to establish a strong data protection regime. This is the paradox concerning the adequacy requirement. The question as to exactly what an assessment of a state's level of data protection should minimally include has not yet been solved. In addition, this assessment is not a prerequisite for all Member States or all data transfers to third states. *A fortiori*, even when the assessment of the adequacy of the data protection regime in the third state is laid down as a requirement, it is not always applied as such.

## How to assess adequacy?

The Additional Protocol to the Data Protection Convention specifies the necessity of an assessment of the level of data protection offered by the receiving third state, but does not specify how to carry out the assessment. According to the Explanatory Report to the Additional Protocol, the provisions of Chapter II (basic principles of data protection) of the Data Protection Convention should be taken into account when assessing the adequacy of the third state's legal framework on data processing. Nonetheless, this clarification is only

valid as far as the Convention's principles are relevant for the specific case of transfer.[8] Thus, the basic principles of data protection do not necessarily have to be considered.

As a consequence, each judicial and law enforcement authority of each Member State could come up with its own concept for assessment of the level of data protection of the receiving third state. Differences in evaluation tools and methods as well as in the items evaluated can result in divergent outcomes, depending on the authority or the Member State carrying out the assessment. From the point of view of the third state requesting personal data from two states that have ratified the Additional Protocol, this can lead to a different reply from each state and exacerbate the risk of *data-shopping*.

The development of a uniform checklist of the minimum provisions necessary for an adequate level of data protection would be an important step. In fact, the groundwork has already been laid. The Article 29 Working Party reflected on the matter and published a discussion document on the central question of adequacy. The document focused on the adequacy requirement in Directive 95/46/EC and was already published in 1997.[9] Even though it is not applicable to the field of criminal matters, the document provides good guidelines on what an adequacy assessment should include. These guidelines have been formulated in a general manner and could have easily been adjusted to fit adequacy assessment in criminal matters.

To allow for some flexibility on the part of the states exchanging data, the Additional Protocol allows for derogations from the adequacy requirement that should be interpreted restrictively.[10] 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. Corresponding to the ECHR, 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 as follows: to protect an important public interest, the exercise or defence of a legal claim, or the extraction of data from a public register. Exceptions 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.[11]

In case an adequate level of data protection cannot be assured, another possibility for exchange still exists if the receiving state provides sufficient safeguards that are deemed adequate by the requested 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.[12]

## Mandatory nature or the lack thereof

The adequacy requirement is not a requirement for all transfers of personal data from a Member State to a third state that is not bound by the Data Protection Convention. Three arguments motivate this statement.

Firstly, the Additional Protocol has so far been ratified by only 16 EU Member States.[13] Even though the Protocol has a general scope and is applicable to all automatically processed personal data, its partial ratification means that the adequacy requirement is not a uniform requirement for all data transfers from the EU to third states.

Secondly, the EU legal instruments including the adequacy requirement are only applicable to a specific group of data transfers. Directive 95/46/EC – which is implemented in every Member State – includes the same adequacy requirement, but is only applicable to data transfers that fall within the scope of Community law. Similarly, Regulation 45/2001[14] – which is also implemented in every Member State – has included a provision on the adequacy requirement, but is only applicable to the transfers of personal data made by Community institutions and bodies. The newest legal instrument in the field of data protection, the Frame-

work Decision on Data Protection in Criminal Matters[15] – which needs to be implemented by all Member States by 27 November 2010 –is equally limited in scope. It is only applicable to the personal data that have been transmitted or made available by another Member State and excludes the data gathered by the requested Member State itself. The Framework Decision states that, in future agreements, the adequacy assessment should be ensured. Still, in accordance with the Framework Decision, Member States can derogate from the adequacy requirement for the protection of specific legitimate interests of the data subject, legitimate prevailing interests – especially important public interests –, or when sufficient safeguards are provided by the receiving state.

Thirdly, the data protection rules that the EU agencies Eurojust and Europol have laid down for themselves, and which govern transfers to third states, are very different from one another. Europol has introduced a four-step approach for reaching a decision on the adequate level of data protection of a third state.[16] With the exception of urgent circumstances,[17] the Management Board consults the Joint Supervisory Board (JSB) regarding the processing of data by Europol. Then, the Council of the EU conducts a second check and, in a third step, the Director initiates negotiations, after which the Management Board and the JSB need to give their approval to conclude the agreement in a final step. This four-step filtering system has no counterpart in Eurojust data protection rules. In accordance with the rules governing data transfers by Eurojust, an adequacy assessment by its data protection officer is sufficient. Eurojust does not involve the Council and only turns to the JSB when the data protection officer meets difficulties in making his assessment. The recent decision on strengthening Eurojust does not add to Eurojust's data protection provisions in order to improve the assessment.

Therefore, the mandatory nature of the adequacy requirement is diverse and depends on which Member State or EU agency is transferring data, whether the state has ratified the Additional Protocol or not, and on the data that are transferred. Obviously, this conclusion is only based on the EU's legal instruments and not on Member States' national law. Member States can – on their own initiative – incorporate an adequacy requirement for outgoing data transfers in their national law.

Only two cases exist in which all EU Member States are obliged to assess the adequacy of the level of data protection in a third state requesting personal data: that in which the processing of data falls within the scope of Community law and that in which the data are processed for the purpose of a criminal investigation, as long as it concerns data that the transferring Member State has received from another Member State. There is thus no general adequacy requirement for data processed for the purpose of prevention, investigation, and prosecution of criminal offences.

## A "forgotten" requirement

Even when there is a clear obligation to make an adequacy assessment, there are cases in which it has been "forgotten". Obviously, the word "forgotten" is meant in an ironic sense here, as it is difficult to imagine mandatory rules accidentally not being applied. It is more likely that a conscious – politically more opportune – choice was made to disregard them. This is especially visible in transatlantic cooperation. The agreements made between the EU and its agencies mandated to deal with cooperation in criminal matters (Eurojust and Europol), on the one hand, and the US on the other, have one particular thing in common. They all ignore the adequacy requirement. As mentioned earlier, both Eurojust and Europol are bound by the adequacy requirement. They are not parties to the Additional Protocol to the Data Protection Convention, but have included the requirement in their own set of rules governing their data transfers to third states.

In the Europol Decision,[18] two possibilities are regulated by which Europol can transfer personal data to third states.[19] The general rule is the conclusion of an agreement, after authorisation of the Council and supported by a prior opinion of the JSB. As an exception, the Director of Europol can enter into negotiations without

authorisation of the Council and without prior consultation with the JSB. Exceptional circumstances are defined – at the discretion of the Director – by the absolute necessity to transmit personal data in order to safeguard the essential interests of the Member States concerned, within the scope of Europol's objectives, or in the interest of preventing imminent danger associated with crime.[20] The Director must in these circumstances consider the level of data protection applicable for the receiving authority in the third state and weigh this against the essential interests. The parameters for making this assessment are laid down in Article 23 of the Europol Decision. In comparison to the Europol Convention, the Europol Decision adds a new parameter: "whether or not the entity has agreed to specific conditions required by Europol concerning the data."[21] This is a useful and necessary guideline for the Director. However, the provision of parameters to judge the adequacy of the level of data protection of a third state could have been developed into a more detailed checklist. Also, in the case of Europol, the question of what should be minimally included in an adequacy assessment has been left open.

The exceptional way for Europol to negotiate data transfers to third states – through the Director, without authorisation of the Council – was used to conclude two agreements with the US after the 2001 terrorist attacks.[22] The first of these agreements was, however, inserted into the conventional procedure at the Council meeting on Justice, Home Affairs and Civil Protection.[23] The Director of Europol was then authorised to conclude a cooperation agreement on the exchange of strategic information, not including personal data, the negotiations on which had already begun.[24] During this same Council meeting, Europol received the authorisation to start negotiations on another agreement that would focus on the exchange of personal data. This would mean that the level of data protection of the US should be assessed in accordance with Article 18, §1, 2) of the Europol Convention (which was applicable at the time) and in accordance with the rules governing the transmission of personal data by Europol to third States and third bodies.[25] The Council noted during this meeting that a data protection report concerning the US had been drawn up by Europol.[26] Nonetheless, the JSB stated that Europol did not provide a report on the data protection law and practice in the US and that the JSB was therefore unable to make a conclusion on the level of data protection in the US.[27] On 3 October 2002, the JSB issued another opinion based on practical experiences with the US system and on presentations made during the negotiations.[28] The JSB stated that the Council was in the position to allow the Director of Europol to conclude the agreement, but expressed concerns about the purposes for which personal data would be used after their exchange to the US. Data should not be used for purposes outside the objectives of Europol. These concerns are not unreasonable since the purposes for which the data can be used in accordance with the Agreement have been widened by the parties in documents called "exchange of notes". These notes are not formally part of the Agreement, but are intended to assist its implementation.[29] Nonetheless, they explicitly state that the data that are exchanged in accordance with the Agreement can also be used for "*inter alia, 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.*"[30] Immigration investigations and confiscation not based on a criminal conviction clearly go further than the objectives of Europol.

Still, the 2002 Supplemental Europol-US Agreement on the exchange of personal data and related information (2002 Europol-US Agreement) was signed on 6 November 2002. Proof of the US endorsing a data protection regime that fulfils the conditions of the adequacy requirement has not been produced to date. An informal explanatory note only reflecting Europol's view on the 2002 Europol-US Agreement, states, quite sarcastically, that the Agreement is "*generally in line with the major principles incorporated in Europol's legal framework*". The adequacy requirement does not seem to be considered a major principle of Europol's legal framework. The text of the note goes even further and states that the provisions of Article 5 of the Agreement on general terms and conditions "*would not be used as a legal basis for generic restrictions, but only in specific cases where there was a real necessity.*"[31] The phrase "generic restrictions" can clearly be understood

as the requirement involving an adequate level of data protection. This means that the note calls for the rejection of this requirement in the cooperation with the US.

The exception that has been made for the US could create political strife with other third states. Europol has negotiated agreements with Australia, Canada, Croatia, Iceland, Norway, and Switzerland. All of these agreements were negotiated after an opinion of the JSB was issued and confirmed by the Council that no obstacles exist to include the transmission of personal data in the agreement. The only exception that has been made so far is for the US.

Eurojust only exchanges case-related[32] personal data with third states bound by the Data Protection Convention or third states that support an adequate data protection system. In the latter case, possible additional safeguards can be included in agreements between the data controller and the third state.[33] Switzerland, Iceland, Romania, Norway, and Croatia all have ratified the Data Protection Convention. The US was the first state not bound by the Data Protection Convention to conclude an agreement with Eurojust. In fact, proof of an adequacy assessment of the US rules on data protection was not provided. Instead, the Eurojust JSB – which is responsible for monitoring data protection – remarkably preferred not to be involved directly in the negotiation process, but instead to be closely informed about the important steps and developments made.[34] The JSB expressed concerns regarding the use of data that had been made public regardless of whether the release had occurred lawfully or not.[35] The lack of an assessment on the level of data protection was not mentioned.

With regard to the inclusion of the adequacy requirement in the cooperation agreements, the Agreement concluded between the EU and the US on mutual legal assistance[36] and the Agreement concluded between Eurojust and the US[37] can be analysed together. The requirement has, in fact, been abolished in these instruments even more clearly than in the 2002 Europol-US Agreement. Both Agreements include an article on "limitations on use to protect personal and other data," which explicitly states that generic restrictions with respect to the legal standards of the requesting State or party in the processing of personal data may not be imposed by the requested State or party as a condition for providing evidence or information.[38]

Where, in the 2002 Europol-US Agreement, the US was labelled an adequate partner with regard to its data protection regime, even though this was unjustified, in the 2003 EU-US Agreement and the 2006 Europol-US Agreement, the adequacy requirement was thrown overboard.

# Continuing Along the Same Path

Four years after it was revealed that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) answered to administrative subpoenas issued by the US Department of the Treasury (UST) by sending personal data (financial messaging data) in bulk for the purpose of investigating the financing of terrorism under the Terrorist Finance Tracking Programme (TFTP), the US called for an agreement with the EU on a regular transfer of these data. A change in SWIFT's architecture meant that a large amount of its data was no longer stored in the US, but in the EU. Thus, in 2009, the US and the Council of the EU began negotiating an agreement in order to establish the transfer of SWIFT's financial messaging data for the purpose of the TFTP. First, a temporary agreement of nine months – the Interim Agreement – was to be signed and, after that, a permanent agreement negotiated. However, the entry into force of the Lisbon Treaty made the European Parliament's consent a prerequisite for entry into force of the Interim Agreement. A substantial report written by Parliament Member Jeanine Hennis-Plasschaert[39] brought about the rejection of the Interim Agreement on 11 February 2010.[40] Not mentioned in the report as a reason to vote against the Interim Agreement, but nevertheless important, is Article 6, in which it is stated that the UST is "*deemed to ensure an adequate level of data protection*". The Article 29 Working Party and the Working Party on Police and Justice rightfully ex-

pressed their disapproval of this provision and pointed out that other reports (that are confidential, such as the report by Judge Bruguière on the compliance of the TFTP with the safeguards offered by the UST) cannot necessarily substitute an adequacy assessment.

# Adequate Perplexity

Research has proven that the basic data protection principles applicable in criminal matters in the EU are not fully complied with in the cooperation between the EU Member States.[41] In much the same way as this internal exchange and its lack of duly applied data protection principles, compliance with the adequacy requirement is also problematic. In the external exchange of personal data between EU Member States and third states, the adequacy requirement is not a general requirement and has not been defined in detail. Differences between Member States' views on an adequacy check can thus lead to *data shopping* or the search by a requesting third state for the most "lenient" Member State. Therefore, the meaning of the requirement itself can be put into question. If you do not operate with the same criteria, why do you have the requirement in the first place? The answer should be to protect personal data transferred to third states that might have a different view on data protection than that represented by EU data protection principles. However, the protection that the adequacy assessment should offer is clearly not watertight.

Considering the major importance of the protection of personal data transferred for the purpose of a criminal investigation or prosecution, and also considering the high importance of the protection of personal data transferred to a state that has not ratified the Data Protection Convention, it is all the more surprising to see that the assessment intended to ensure this protection is not mandatory in the EU.

From a political point of view, it is also surprising to see the clear difference in the treatment of third states. The exception that has been made for the US of not carrying out an adequacy assessment has not been made for any other third state so far.

It is therefore understandable that the members of the Article 29 Working Party and the Working Party on Police and Justice reacted to the lack of an adequacy assessment in the Interim Agreement with an appropriate degree of perplexity. This degree of perplexity is equally justified with regard to the agreements that the EU, Europol, and Eurojust concluded with the US authorities.

Looking at the future of the adequacy requirement, the mandate that has been adopted to launch negotiations between the Commission and the US authorities on a new agreement for the transfer of financial messaging data includes the statement that the Agreement shall contain safeguards and controls, which ensure an adequate level of protection of personal data.[42] Even though this is a general statement that is in need of further clarification as to which safeguards and controls will be provided, it is sure to trigger less perplexity on the part data protection experts.

---

1. Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS no. 108, 28 January 1981.↩
2. So far, 14 third states have ratified the Data Protection Convention.↩
3. Chronologically, it was Directive 95/46/EC (*O.J.* L 281, 23 November 1995, pp. 31-50) that was the first instrument to include the adequacy requirement; however, the scope of the Directive is limited to the processing of personal data for the purpose of activities that fall within the scope of Community law.↩
4. 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, 8 November 2001.↩
5. See, e.g., Directive 95/46/EC, *O.J.* L 281, 23 November 1995, pp. 31-50.↩
6. See, e.g. Article 26, Council of the European Union, Rules of procedure on the processing and protection of personal data at Eurojust, *O.J.* C 68, 19 March 2005, pp. 1-10 and Article 4, Council of the European Union, Act 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies, *O.J.* C 88, 30 March 1999, pp. 1-3.↩
7. See also European Data Protection Supervisor, Third opinion 27 April 2007 on the Proposal for a Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters, *O.J.* C 139, 23 June 2007, § 26.↩

8. Additional Protocol to the Data Protection Convention, ETS no. 181, 8 November 2001, Explanatory Report, § 29.↩
9. Article 29 Data Protection Working Party, XV D/5020/97-EN final, WP 4, 26 June 1997.↩
10. Additional Protocol to the Data Protection Convention, ETS no. 181, 8 November 2001, Explanatory Report, ETS no. 181, 8 November 2001, Explanatory report, §31.↩
11. Ibid., §31.↩
12. Ibid., § 32-33.↩
13. The protocol entered into force for Austria, Cyprus, Czech Republic, Estonia, Ireland, Germany, Hungary, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, and Sweden.↩
14. European Parliament and Council, Regulation (EC) no. 45/2001, 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *O.J.* L 8, 12 January 2001, pp. 1-22.↩
15. Council of the European Union, Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *O.J.* L 350, 30 December 2008, pp. 60-71.↩
16. Council of the European Union, Decision of 27 March 2000 authorising the Director of Europol to enter into negotiations on agreements with third States and non-EU related bodies, *O.J.* C 106, 13 April 2000, pp. 1-2.↩
17. In urgent circumstances, the Europol Director is authorized to transmit personal data to third states.↩
18. Council Decision establishing the European Police Office, *O.J.* L 121, 15 May 2009, pp. 37-66.↩
19. Council of the European Union, Act 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies, *O.J.* C 88, 30 March 1999, p. 1.↩
20. Article 2, §1, b) Council Act of 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies. The inclusion of terrorist offences is a new addition to this provision made by the Europol Decision.↩
21. Article 23, §9, e) of the Europol Decision.↩
22. V. Mitsilegas, "The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data," *EFAR* 2003, vol. 8, pp. 516-517.↩
23. European Council, 14581/01, 6-7 December 2001, p. 11.↩
24. The first draft, dating from 31 October 2001, is available in the Council of the EU's public documents database. Council of the European Union, 13359/01, Draft agreement between Europol and USA, 31 October 2001.↩
25. *O.J.* C 88, 30 March 1999, p. 1.↩
26. European Council, 14581/01, 6-7 December 2001, p. 11.↩
27. Europol JSB, Document 01/38, 26 November 2001, p. 2.↩
28. Europol JSB, Document 02/65, 3 October 2002.↩
29. Council of the European Union, 13696/1/02, 28 November 2002, p. 2.↩
30. Council of the European Union, 13996/02, 11 November 2002, p. 3.↩
31. Council of the European Union, 13696/1/02, 28 November 2002, p. 10.↩
32. Evidently, with regard to non case-related data exchange, the issue of an adequate level of data protection or adherence to the 1981 CoE Convention is not pressing as, in this respect, use for a wider range of purposes is allowed.↩
33. Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, *O.J.* L 63, 6 June 2002, Article 27, §4 and Council, Rules of procedure on the processing and protection of personal data at Eurojust, *O.J.* C 68, 19 March 2005, Article 28, §§ 2 and 3.↩
34. Joint Supervisory Body of Eurojust, Activity Report 2006, p. 6, www.eurojust.europa.eu↩
35. Ibid., pp. 6-7.↩
36. Agreement 25 June 2003 on mutual legal assistance between the European Union and the United States of America, *O.J.* L 181, 19 July 2003, p. 41.↩
37. Agreement between Eurojust and the United States of America, 6 November 2006, www.eurojust.europa.eu.↩
38. Article 9 of the 2003 EU-US Agreement and Article 9 of the 2006 Eurojust-US Agreement.↩
39. European Parliament Recommendation, A7-0013/2010, 5 February 2010.↩
40. *O.J.* L 8, 13 January 2010, p. 9.↩
41. E. De Busser, Data protection in EU-US criminal cooperation, Antwerp-Apeldoorn, Maklu, 2009, pp. 127-183.↩
42. Recommendation from the Commission to the Council, SEC(2010)315 final, 24 March 2010.↩

COPYRIGHT/DISCLAIMER
© 2026 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other

contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

## About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union