European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers

Alexander Zinser*

Data transfers out of the European Union are only admissible in cases where the third country in question ensures an adequate level of protection. The European Data Protection Directive sets out the legal basis for the procedures used to determine the adequacy of these protections and the relevant findings of the European Commission. Problems derived from the wording of the European Data Protection Directive, however, are that the data protection authorities are not aware of a data transfer to a third country in all cases, and that there is not an explicit power to stop data transfers as soon as proceedings are opened. It is desirable that data controllers will be granted a certain time-limit within which they could work on safeguards to ensure the adequate level of protection.

I. INTRODUCTION

International data transfers, either between the European Union Member States or out of the European Union, are regulated by Directive 95/46/EC, which relates to the processing of personal data and the free movement of data (Directive).[1] The Directive applies "to the processing of personal data wholly or partly by automatic means," and to the manual processing "of personal data which form part of a filing system or are intended to form part of a filing system."[2] The Directive defines personal

* Dr. jur.; Senior Attorney at Agilent Technologies Deutschland GmbH, Böblingen, Germany, a subsidiary of Agilent Technologies Inc., Palo Alto, California. The views expressed in this Article are the author's own and do not necessarily reflect those of Agilent Technologies.

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Data; Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter Council Directive].

2. *Id.* art. 3(1), at 39.

data as "any information relating to an identified or identifiable natural person ('data subject')."[3] "This may include the individual's e-mail address, Internet provider (IP) number, information collected by cookies . . . as well as any other features that would enable the identification of an individual."[4] According to the Directive, an identifiable person is a person "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[5] Also, processing of personal data is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[6] The definition in the Directive is wide, but nonexhaustive.

By harmonizing data protection laws, the Directive ensures the movement of personal data without restrictions within the European Union. Member States are not allowed to restrict the freedom of transfer of personal data by arguing that another Member State does not have an adequate level of data protection.[7] Furthermore, the Directive allows data controllers to process personal data concerning citizens residing anywhere in the European Union.[8] Equivalent principles can be seen in the freedom of movement of goods, services, capital and persons.[9]

The Directive also regulates the transfer of data out of the European Union. According to article 25(1) of the Directive, such a transfer is only admissible if an adequate level of data protection is secured in the recipient country.[10] Because it is not clear what is meant by the formula "adequate level of protection," there is the risk that different applications will occur within the European Union Member States. The data controller could potentially choose, for the export of data, the country with the low-

---

3. *Id.* art. 2(a), at 38.

4. Tanguy van Overstraeten & Emmanuel Szafran, *Data Protection and Privacy on the Internet: Technical Considerations and European Legal Framework*, 7(3) COMPUTER TELECOMM. L. REV. 56, 59 (2001).

5. Council Directive 95/46, art. 2(a), at 38.

6. *Id.* art. 2(b), at 38.

7. *See* David I. Bainbridge, *Processing Personal Data and the Data Protection Directive*, 6 INFO. & COMM. TECH. L. 17, 18 (1997).

8. *See* Dag Wiese Schartum, *Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects*, 15 INT'L. REV. L. COMPUTERS & TECH. 157, 158 (2001).

9. *See* DAVID I. BAINBRIDGE, THE EC DATA PROTECTION DIRECTIVE 42 (1996).

10. *See* Council Directive 95/46, art. 25(1), at 44.

est level of data protection.[11] It is for this reason that the Directive provides for a harmonized practice of decision making. The Directive provides a basis from which the European Commission can determine whether a third country ensures an adequate level of data protection.[12]

II. DATA TRANSFER TO THE UNITED STATES

With regard to the United States, the European Commission adopted the Decision on Safe Harbor whereby "the . . . safe harbor privacy principles . . . implemented in accordance with the guidance provided by the Frequently Asked Questions . . . are considered to ensure an adequate level of protection for personal data transferred from the European Union to organizations established in the U.S."[13] The idea is that both the Safe Harbor Privacy Principles issued by the United States Department of Commerce on July 21, 2000,[14] and the accompanying Frequently Asked Questions[15] set forth the provisions ensuring the adequate level of data protection. Both the Safe Harbor Principles and the Frequently Asked Questions are legally binding.[16] It is not the intention that the Safe Harbor Principles affect U.S. law, but rather to provide a so-called "safe harbor" to companies in respect to the Directive. Technically, U.S. companies have no obligation to adhere to the Safe Harbor Principles. Businesses are asked to do so to avoid any adverse effects with regard to data transfers between the European Union and the United States.[17] However, it remains to be determined whether the relevant procedural provisions on international data transfer of the Directive are adequate.

---

11. *See* Kees Jan Kuilwijk, *Recent Developments in E.U. Privacy Protection Regulation*, 6 INT'L TRADE & REG. 200, 201 (2000).

12. *See* ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE: KOMMENTAR 275 (1997).

13. Art. 1 of the Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the European Commission on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce, [2000] O.J. L215/7, *at* http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm (last modified May 7,2003).

14. U.S. Department of Commerce, *Safe Harbor Privacy Principles* (2000), *at* http://www.export.gov/safeharbor/shprinciplesfinal.htm.

15. *Id.*, *Safe Harbor Documents*, *at* http://www.export.gov/safeharbor/sh_documents.html under the heading "C. Frequently Asked Questions (FAQs)".

16. *See* Heather Rowe, *Data Protection*, IT LAW TODAY 7.10(4) (1999).

17. *See* Gregory Shaffer, *The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice*, 5 EUR. L.J. 419, 423 (1999).

III. MUTUAL INFORMATION

The basis for a uniform practice is that a mutual and timely information flow takes place between the Member States and the European Commission. Therefore, the Directive provides that "the Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection."[18]

The above-mentioned "cases" are those which occurred in the past or will occur in the future. Furthermore, they need to refer to the adequacy requirement according to article 25(1) of the Directive.[19] The mutual information does not need to take place where the transfer is based on one of the exceptions as set out in article 26(1) of the Directive.[20] These derogations are:

> (a) the data subject has given his consent . . . (b) the transfer is necessary for the performance of a contract . . . (c) the transfer is necessary for the conclusion or performance of a contract . . . (d) the transfer is necessary or legally required on important public interest grounds . . . (e) the transfer is necessary in order to protect the vital interests of the data subject.[21]

It has been argued that information must also flow in cases where one of the stated exceptions apply.[22] In these cases, however, the adequacy of protection is not *a priori*, with the result that sharing mutual information seems not to be necessary. The rights of the data subjects are not so at risk that such an information sharing would not foster protection of the data subjects in question. From a practical point of view, the number of the cases would be without limits, and, without having further resources, it would be hard to follow all cases which have been reported.

The Member States must have detailed knowledge of the situation in their territory; otherwise, they are not able to fulfill their duty of information properly. The Directive does not really help in this respect. It is acknowledged that the controller must notify the supervisory authority of any proposed transfer of data to third countries.[23] However, there are various simplifications of or exemptions from the notification so that a complete notification of data transfers to third countries is not secured.[24]

---

18. Council Directive, 95/46, art. 25(3), 1995 O.J. (L 281) 31, 46.
19. *Id.* art. 25(1), at 45.
20. DAMMANN & SIMITIS, *supra* note 12, at 276.
21. Council Directive 95/46, art. 26(1)(a)-(e), at 46.
22. *See* OLIVER DRAF, DIE REGELUNG DER ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER NACH ART. 25, 26 DER EG-DATENSCHUTZRICHTLINIE 100 (1999).
23. *See* Council Directive 95/46, art. 19(1)(e), at 46.
24. *See id.* art. 18(3), at 44.

With regard to the Safe Harbor arrangement, a list of all organizations that register through the website or through a letter[25] is maintained by the United States Department of Commerce.[26] The list shows the organizations which adhere to the Safe Harbor principles.[27] Therefore, the national data protection authorities in the European Union have some information that could help to identify organizations that are not self-certified for Safe Harbor. They could approach international non-Safe Harbor companies based in Europe and the United States and ask them how they fulfill the requirement of adequacy. This could be a mechanism to gain information on the fulfillment of the adequacy requirement.

IV. NONEXISTENCE OF AN ADEQUATE LEVEL

Regardless of whether an information source is in connection with a data transfer to a third country, the European Commission has to decide whether the relevant third country can ensure an adequate level of data protection.[28] In cases in which the European Commission finds "that a third country does not ensure an adequate level of protection . . . Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question."[29] It is unclear what kinds of measures are envisioned to prevent the relevant data transfer. Presumably, telecom operators would be asked to intervene and block any transfer.[30]

Before the European Commission makes a decision, a committee composed of representatives of the Member States has to be involved: the European Commission "shall submit to the committee a draft of the measures to be taken," and "[t]he committee shall deliver its opinion on the draft."[31] Also, the European Commission has to ask the working party[32] for "an opinion on the level of protection in the Community and in third countries."[33]

---

25. U.S. Dep't of Commerce, *Safe Harbor List*, *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Nov. 18, 2003).

26. U.S. Dep't of Commerce, *Safe Harbor Workbook*, *at* http://www.export.gov/safeharbor/sh_workbook.html (last updated Nov. 13, 2003).

27. *See* U.S. Dep't of Commerce, *Safe Harbor List*, *supra* note 25.

28. *See* Council Directive 95/46, art. 25(1), at 45.

29. *Id.* art. 25(4), at 45-46.

30. *See* Kuilwijk, *supra* note 11, at 202.

31. Council Directive 95/46, art. 31(2), at 49.

32. According to article 29(1)-(2) of the Directive, the working party shall have advisory status and act independently. It is composed of representatives of the supervisory authority, which each Member State is required to establish. *See id.* art. 29(2), at 48.

33. Council Directive 95/46, art. 30(1)(b), at 48.

The decision of the European Commission binds the Member States.[34] The latter have to take the appropriate measures to prevent such a data transfer.[35] As a result, the data transfer of the highest economic importance can be forbidden.[36] Authors in the United States of America are very doubtful about the possible results.[37] From my point of view, a practical solution would be for data controllers to be granted a certain time limit within which they have to mitigate the situation. This would allow data controllers to find a solution without having any adverse effects on their economic situation.

The provisions indicate that a general assessment has to be made. However, these decisions are difficult. A comprehensive regulation of data protection is not in existence in many countries. In some countries only the public sector is regulated, whereas in others, data protection laws govern only the private sector. A further problem could be the federal structure of many countries. Rules may differ between the local states and it could be impossible to determine whether the relevant country has adequate protection. Moreover, from a political and diplomatic point of view, it could cause sufficient problems warranting the placement of a country on a "black list."[38] Overall, the provisions could cause difficulties and uncertainties.

Therefore, it is desirable that the Directive state the criteria for the determination of the adequacy requirement. With regard to the overwhelming objective of the Directive, in my opinion, the criteria should be as follows: (1) lawfulness of the processing of personal data; (2) special protection of sensitive data; (3) rights of the data subjects; (4) security of processing and (5) control and enforcement measures. The criteria are mentioned in the Directive, and they ensure that the objective of the Directive is secured. It has yet to be reviewed whether and how the criteria are regulated in the data protection laws of the country to which the data is transferred.[39]

---

34. Treaty Establishing the European Community, art. 110, 1997 O.J. (C 340) 3.

35. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 486-87 (1995).

36. *See id.* at 486.

37. *Id.*

38. *See* Peter Blume, *Transborder Data Flow: Is There a Solution in Sight?*, 8 INT'L J. L. & INFO. TECH. 65, 70 (2000).

39. *See* Alexander Zinser, *International Data Transfer Out of the European Union: The Adequate Level of Data Protection According to Art. 25 of the European Data Protection Directive*, 22 JOHN MARSHALL J. COMPUTER & INFO. L. (forthcoming 2003).

V. REMEDY OF THE SITUATION

Where adequate levels of protection do not exist, the European Commission "shall enter into negotiations with a view to remedying the situation."[40] The Directive does not describe the method of remedying the situation. However, the aim is clear: the third country in question has to achieve an adequate level of protection.[41] Normally, the situation will be resolved by negotiations. Possibly, the result could be an agreement whereby the third country is obliged to ensure or to provide for an adequate level of protection. However, it makes sense that the Directive does not state the parties nor the content of the negotiations. The European Commission should be free to decide the details of the negotiations depending on the situation in question.

VI. EXISTENCE OF AN ADEQUATE LEVEL

After involving the committee[42] and the working party,[43] the European Commission may find "that a third country ensures an adequate level of protection . . . by reason of its domestic law or of the international commitments it has entered into."[44] So far, the European Commission has recognized Switzerland,[45] Hungary,[46] and Canada[47] as providing adequate protection. With regard to data transfers out of the European Union to the United States, the European Commission adopted a decision regarding the United States Department of Commerce's Safe Harbor privacy principles and related Frequently Asked Questions as an adequate level of protection.[48]

---

40. Council Directive 95/45, art. 25(5), 1995 O.J. (L 281) 31, 46.
41. *See id.* art. 25(1), at 45.
42. *See id.* art. 31(2), at 49.
43. *See id.* art. 29, at 48.
44. *Id.* art. 25(6), at 46.
45. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, 2000 O.J. (L 215) 1, *at* http://europa.eu.int/comm/internal_market /en/dataprot/adequacy/ch_00-518_en.pdf.
46. Commission Decision 2000/519/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, 2000 O.J. (L 215) 4, *at* http://europa.eu.int/comm/internal_market/en /dataprot/adequacy/hu_00-519_en.pdf.
47. Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002 O.J. (L 2) 13, *at* http://europa.eu.int/comm/internal_market/en/dataprot/adequacy /canadadecisionen.pdf.
48. *See* Commission Decision 2000/520, *supra* note 13.

The Directive does not state the consequences for the Member States with regard to the European Commission's findings. Clearly, the level of data protection should not be an obstacle for a data transfer. In contrast to the data flow between Member States,[49] there is not a duty to approve the data transfer. The European Commission merely determines that there is an adequate level of protection.[50] However, it is up to the national data protection laws to define the legal consequences of the European Commission's finding. The relevant national law can provide that the data transfer cannot be prohibited any longer. However, this is not a consequence clearly stated in the Directive.[51] It would be more desirable if the Directive clearly stated that data transfers to third countries, recognized by the European Commission as having an adequate level of protection, would be lawful.

VII. CRITICISM AND CONCLUSION

The Member States have to ensure that they will become aware of an export of data in a third country in which the adequate level of protection has been questioned. In connection with the duty to notify public authorities, a proposed transfer of data to third countries has to be stated.[52] However, there are also various provisions which provide for a simplification of or even exemption from the notification.[53] In all of these cases, the relevant public authority may not be aware of a data transfer to an unsecure country. Overall, the Directive does not specify provisions whereby the public authorities will become aware of such a data transfer. The Directive does not guarantee an effective information flow.

In addition, data transfer can continue to take place even while the European Commission is assessing the level of data protection of the third country in question. It would be advisable that the national data protection authorities take precautions to stop such a transfer as soon as any proceedings have been opened. Before the European Commission comes to the conclusion that the third country does not ensure an adequate level of data protection, a substantial data flow to the relevant third country could have already taken place.

With regard to the data transfer to the United States, the United States Department of Commerce, on behalf of the U.S. Government, and

---

49. Council Directive 95/46, 1995 O.J. (L 281) 31.
50. *Id.* art. 25(1), at 45.
51. *See* DAMMANN & SIMITIS, *supra* note 12, at 280.
52. Council Directive 95/46, art. 19(1)(c), at 44.
53. *Id.* art. 18(2), at 44.

Directorate General XV of the European Commission, negotiated on how to fulfill the adequacy requirement of the Directive. The negotiations lasted more than three years. During that period, there was a lot of uncertainty on the lawfulness of a data transfer to the United States and on possible solutions to ensure an adequate level of protection.[54] Apart from the ability to stop such a data transfer, the national data protection authorities should also have the right to grant data controllers a certain time limit to establish one of the derogations as set out in article 26 (1),[55] or use contractual clauses[56] as a means to fulfill the adequacy requirement. It is important that data controllers will have time available to find a solution. Overall, it can be said that the relevant procedural provisions of the Directive on international data transfer have some weaknesses.

54. *See* Blume, *supra* note 38, at 80-81.

55. *See* Council Directive 95/46, art. 26(1), at 46.

56. *See* Commission Decision 2001/49/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001 O.J. (L 181) 19-31, *at* http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.