UIC John Marshall Journal of Information Technology & Privacy Law

Volume 21
Issue 4 *Journal of Computer & Information Law - Summer 2003*

Article 3

Summer 2003

International Data Transfer Out of the European Union: The Adequate Level of Data Protection According to Article 25 of the European Data Protection Directive, 21 J. Marshall J. Computer & Info. L. 553 (2003)

Alexander Zinser

INTERNATIONAL DATA TRANSFER OUT OF THE EUROPEAN UNION: THE ADEQUATE LEVEL OF DATA PROTECTION ACCORDING TO ARTICLE 25 OF THE EUROPEAN DATA PROTECTION DIRECTIVE

ALEXANDER ZINSER†

I. HISTORY OF THE DIRECTIVE

The European Parliament first took initiatives to introduce Community norms in the field of data protection in the 1970s and passed several resolutions.[1] However, the European Commission blocked them and recommended that Member States should sign and ratify the Council of Europe Convention.[2] Due to the discretion left to the Member States, national data protection laws differed in a significant way. In 1990, the European Commission submitted a number of proposals to foster the free movement of data including proposals on data protection.[3] The reason

† J.D.; 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. Simon Chalton & Shelagh Gaskill, *Data Protection Law* 1150-51 (London Sweet & Maxwell 1988). The resolutions passed by the European Parliament included

(a) that of April 8, 1976, in which it instructed its Legal Affairs Committee to report to it on community activities to be undertaken with a view to safeguarding rights of the individual in the face of developing technical progress in the field of automatic data processing;
(b) that of May 8, 1979, in which it called upon the Commission to prepare a proposal for a directive on the harmonisation of legislation on data protection; and
(c) that of March 9, 1982 . . . in which it called on the member states of the European Community to ratify the Council of Europe Convention.

Id.

2. Council of Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data <http://conventions.com.int/Treaty/en/Treaties/Html/108.htm> [hereinafter Council].

3. Graham Pearce & Nicholas Platten, *Achieving Personal Data Protection in the European Union*, 26 J. Com. Mkt. Stud. 529, 532 (1988).

for these activities was to provide for sufficient harmonization of the national laws, which still varied considerably. Overall, the aim was to complete the Single Market in light of the significant increase in international data transfer.[4] All these activities resulted in the enactment of Directive 95/46/EC ("Directive"), which relates to the processing of personal data and the free movement of data.[5] The Directive mandates significant regulatory controls over business processing and use of personal data.[6] The Member States were required to implement the Directive within three years, by October 24, 1998.[7] Apart from these implementation measures, certain provisions may be deemed to have a direct effect.[8]

II. SCOPE OF THE DIRECTIVE

The Directive shall apply 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.[9] According to the definition stated in the Directive, personal data shall mean "any information relating to an identified or identifiable natural person ('data subject')."[10] This can include the individual's e-mail address, IP number, information collected by cookies, as well as any other information that would enable the identification of an individual.[11] An identifiable person is defined as 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."[12] 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,

4. Peter Malanczuk, *The European Directive on Data Protection and the U.S. "Safe Harbor" Principles - E-Commerce and the Settlement of an International Trade Dispute*, Law of Int'l. Business and Dispute Settlement in the 21st Century, 497, 501 (Carl Heymanns Verlag KG 2001).

5. Directive 95/46/EC.

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

7. *See* David Bainbridge, *EC Data Protection Directive* 54-57, 63-64 (Butterworths 1996).

8. Malanczuk, *supra* n. 4, at 504.

9. Directive 95/46/EC art. 3(1).

10. Directive 95/46/EC art. 2(a).

11. Tanguy Van Overstraeten & Emmanuel Szafran, *Data Protection and Privacy on the Internet: Technical Considerations and European Legal Framework*, 7 Computer Telecomm. L. Rev. 56, 59 (2001).

12. *Id.*

> use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[13]

The definition in the Directive is broad, and even then, non-exhaustive. Particularly, "storage" is also covered, whatever that means. Presumably, the term should be "storing" or "having in store." If the latter, this would have serious consequences for organizations with large quantities of archived information.[14] However, it does not change the position that the focus in the Directive is on the flow of information rather than on the storage of information.[15]

III. DATA TRANSFER TO A THIRD COUNTRY

A. INTRODUCTION

The relevant provision with regard to a data transfer to a third country says:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.[16]

The conclusion which can be drawn from the wording of this provision is that any transfer of data to a third country is unlawful unless an adequate level of protection is secured. This is also made clear by the relevant Recital which states: "Whereas, on the other hand, the transfer of personal data to a third county which does not ensure an adequate level of protection must be prohibited."[17] The Directive does not answer the question what the phrase "ensures an adequate level of protection" implies.[18] The meaning of "transfer of personal data" and "adequate level of protection" needs to be clarified.

B. TRANSFER TO A THIRD COUNTRY

A "transfer" - in the meaning of the Directive - is any procedure whereby data will be transferred outside the European Union. It is irrelevant who transfers the data. For example, a transfer, which will be

---

13. Directive 95/46/EC art. 2(b).

14. David Bainbridge, *Processing Personal Data and the Data Protection Directive*, 6 Info. & Communs. Tech. L. 17, 19 (1997).

15. Dag Elgesem, *The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*, Ethics and Information Technology 283, 284 (1999).

16. Directive 95/46/EC art. 25(1).

17. Directive 95/46/EC Recital (57).

18. Peter Blume, *Transborder Data Flow: Is There a Solution in Sight?*, 8 Intl. J. L. & Info. Tech. 65, 69 (2000).

made to persons responsible for Internet Web sites of the transferor, are also within the scope of the Directive. A transfer to a third country will occur when data will be submitted out of the territory of the European Union. So, a transfer to an embassy situated in a third country will not be within the scope, as the relevant national law will apply to embassies according to international law.[19]

IV. ADEQUATE LEVEL OF PROTECTION

A. INTRODUCTION

A transfer of data to a third country may only occur if an adequate level of protection is ensured. Therefore, if the third country has the same adequate level of protection, a transfer would be lawful. The notion of "adequacy" has to be examined through a case-by-case, pragmatic and functional approach.[20] However, the Directive provides some derogations allowing that a transfer of data to a third country which does not ensure an adequate level of protection may take place if: 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 of a contract; d) the transfer is necessary or legally required on important interest grounds; e) the transfer is necessary in order to protect vital interests of the data subject.[21] However, the mentioned exceptions are not part of this article. The primary focus of this article is to consider the issue of "adequate level of protection." The following sections will assess the relevant criteria.

B. CRITERIA OF THE ADEQUACY

1. *Introduction to the Criteria of the Directive*

The Directive lays down certain criteria for the assessment of the adequacy:

> the adequacy shall be assessed in the light of all circumstances surrounding a data transfer operation, particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectional, in force in the third country in question and the professional rules and

19. Alfonso-Luis Calvo Caravaca & Javier Carrascosa Gonzales, *International Data Protection, Privacy, and Directive 95/46/EC*, Aufbruch nach Europa: 75 Jahre Max-Planck-Institut für Privatrecht 167, 178 (2001).

20. Yves Poullet, Sophie Louveaux & Maria Veronica Perez Asinari, *Data Protection and Privacy in Global Networks: A European Approach*, 8 Elec. Data Interchange L.R. 147, 163 (2001).

21. Directive 95/46/EC art. 26(1).

security measures which are complied with in that country.[22]

The article directs us to ascertain a list of items relating to hard and soft law and to the data transfer itself.[23]

The list is not exclusive. Additional criteria could be taken into account. The criteria can be divided into two parts: firstly, criteria describing the character of the transfer like nature of the data, purpose and duration of the processing operation, country of origin, and country of final destination. Secondly, criteria assisting the assessment of the third country's level of protection like rules of law, professional rules and security measures are crucial. The conclusion can be drawn that a two-fold assessment has to be conducted: firstly, the character of the transfer needs to be established; secondly, a comparison of the level of protection between the two countries needs to be undertaken.[24]

2. *Nature of the Data*

The necessity of protection depends on the nature of the data. The Directive has implemented this by the differentiation between non-sensitive and sensitive data. The latter are data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" and data "concerning health or sex life."[25] However, it must be clear that additional criteria have to be taken into account depending on the relevant situation and/or case. In all instances, an assessment on the sensitivity needs to be conducted.

3. *Purpose of the Processing*

The interpretation of the purpose of the processing can be strict or liberal. In the case that the transferor has transferred the data for a defined purpose, this would bind the transferor. And, any processing which goes beyond the defined purpose should be excluded. However, any defined purpose could be subject to interpretation so that it would not be an exact measure in any case to exclude data transfer, which is not covered by the purpose. Therefore, the purpose must be defined explicitly and exactly in order to mitigate any risks.

The purpose of processing is correlative with the principles relating to data quality. As stated in the Directive, personal data must be "collected for specified, explicit and legitimate purposes and not further

22. Directive 95/46/EC art. 25(2).

23. Francis Aldhouse, *The Transfer of Personal Data to Third Countries Under EU Directive 95/46/EC,* 13 Intl. Rev. L. Computers & Tech. 75, 76 (1999).

24. *See* Brühann, A 30, *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr*, Art. 25 Rdnr. 11, in: Grabitz/Hilf (editors), Das Recht der Europäischen Union (2002).

25. Directive 95/46/EC art. 8(1).

processed in a way incompatible with those purposes."[26] The idea of this provision is to ensure transparency, but it is also controversial as it limits the freedom of the controller.[27] Apart from that, the provision is also motivated by considerations based on the principle of fairness. It would be unfair if the data subject had been given the responsibility of controlling the quality of the data.[28] Also, personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[29] Similar principles can be found in the Convention of the European Council.[30] These principles are one of the keystones of any data protection regulation in general and of the Directive in particular.[31] It makes sense to include the criterion in any assessment of the adequacy of data protection.

4. *Duration of the Processing*

One of the criteria to be taken into account is the planned duration of the processing. It is clear that any processing which is limited to a few hours could be less critical than a processing which takes place over a few years. When processing of data takes place over a few hours, and where the data is subsequently deleted, the data subjects may be deprived of their rights to access to data[32] and to object.[33] In this case, the criterion "duration of processing" is less substantial.

The criterion is mirrored in the general principle of the Directive that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected."[34] It is conclusive that the same general principles should be found in any data protection regulation of a third country.

5. *Country of Origin and of Final Destination*

With regard to the country of origin, cases would be covered where data are not created within the European Union. If these kind of data will be transferred out of the European Union, the protection deviated out of the Directive did not originally apply. Also, the criterion could be taken where foreign companies process data within the European Union.

---

26. Directive 95/46/EC art. 6(1)(b).

27. Blume, *supra* n. 18, at 66.

28. Elgesem, *supra* n. 15, at 284.

29. Directive 95/46/EC art. 6(1)(c).

30. Art. 5 of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

31. Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie*, Kommentar 139 (1997).

32. Directive 95/46/EC art. 12.

33. Directive 95/46/EC art. 14.

34. Directive 95/46/EC art. 6(1)(e).

The Directive is based on the principle of territoriality. It means that the data protection law of the Member State must be observed whenever data are processed in the relevant Member State. It is not relevant whether the data subject is a European Union resident. The relevant contact for the application of the relevant data protection law is the processing of data within a Member State. It is furnished by the Directive, which states "any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States."[35] However, when the same controller is established in several Member States, the necessary measures must be taken to ensure that each of these establishments complies with the applicable national law.[36]

The country of destination is especially crucial in cases where the data will be transferred out of the European Union to more than one country. The data protection laws are not only applicable to the first recipient but are applicable to all recipients. It is for this reason that the final country of destination has to be considered when assessing the adequate level of protection.[37]

6. *Rules of Law*

The expression "rules of law" clarifies that the whole body of law is crucial regardless of the nature of the legal provisions. In Europe, general provisions supported by sectional provisions mainly govern data protection. In non-European Union countries, generally speaking, sectional provisions govern the field of data protection.[38]

Also, the regulations, which have to be taken into account for the assessment of the adequate level of protection, are not limited to a special field of law. Therefore, all provisions can stem from constitutional, criminal, civil, or other fields of law.

The membership in the European Council, United Nations or OECD does not allow the conclusion that national data protection laws are in place. None of the international agreements concluded are directly applicable so that an individual cannot enforce them. It is crucial whether and in which way these international agreements have been implemented in the Member States. However, it can be assumed that states, which have ratified the Council of Europe Convention,[39] have adopted an

35. Directive 95/46/EC Recital (18).

36. Overstraeten, *supra* n. 11, at 59.

37. Dammann, *supra* n. 31, at 274.

38. Oliver Draf, *Die Regelung der Übermittlung Personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie* 80 (1999).

39. Council, *supra* n. 2.

adequate level of data protection.[40]

7. *Professional Rules*

The Directive recognizes that some kind of data protection can come from good practices as well as good laws.[41] Apart from that, the Directive deals with the so-called codes of conduct in a separate provision. According to Article 27(1), the "Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States." By encouraging codes of conduct, the Directive adopts the tradition, especially of the United Kingdom.[42]

It has been argued that codes of conduct should not be taken into account for the assessment of an adequate level of data protection. The reasoning was that codes of conduct are not legally binding so that they are not enforceable. Therefore, an adequate level of data protection would not exist in case of the non-existence of data protection laws. Codes of conduct would not be crucial if data protection laws are in force.[43]

However, the mentioned opinion does not reflect the reality. Codes of conduct adapt the data protection laws, which are regularly drafted in a broad way, to the special situations and conditions in a certain branch. Especially in the United Kingdom, codes of conduct are common and are under the supervision of the Data Protection Commissioner.[44] Therefore, codes of conduct can be regarded as a self-binding and established body of law. It is for this reason that codes of conduct should be one of the criteria for the test of adequacy.

8. *Security Measures*

Legal regulations and security measures can achieve the protection of personal data. One without the other would lead to an ineffective and incomprehensive protection. This has been acknowledged by the Directive by stating

> Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data

40. Working party established by Article 28 of Directive 95/46/EC, Preparation of a methodology for evaluating the adequacy of the level of individuals with regard to the processing of personal data, GD XV D/5025/98 of 24 July 1998, p. 11.

41. Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* 32 (Brookings Instn. 1998).

42. Dammann, *supra* n. 31, at 68.

43. *See* Richard Ellger, *Datenexport in Drittstaaten: Rechtslage Nach Dem Geänderten Entwurf der EG-Richtlinie zum Datenschutz*, Computer und Recht 9 (1993).

44. Wuermeling, *Neue Chancen durch Verhaltensregeln im europäischen Datenschutzrecht?*, 7-8 Datenschutzberater 1 (1993).

> against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access in particular where the processing involves the transmission over network, and against all other unlawful forms of processing.[45]

It seems that the Directive covers the transmission over networks crossing countries. At least, the Directive provides for security measures for these countries. The following may happen in rare cases: even if these countries do not have adequate data protection laws in force, it could be possible to agree that an adequate level of protection is in place provided that security measures provide for a safe and secure transmission.

9. *Criticism*

The criteria mentioned in the Directive make sense. The purpose and duration of the processing are main principles of the Directive. Therefore, it is a must that they are also taken into account when assessing the adequate level of data protection of the third country. However, in practice, the purpose of the data raises some problems. It is not unusual that the purpose is written in a vague manner and/or leaves room for interpretation. In these cases, it could be difficult to find out the relevant purpose of the data.

The data transfer may also be triggered by a legitimate interest of the data subject or controller. The conclusion could be drawn that the level of protection should be lower where the data subject or controller has a legitimate or even vital interest in the data transfer. It could be furnished by the Directive's criterion for making data processing legitimate whereby data may be processed only if "processing is necessary for the purpose of the legitimate interests pursued by the controller or by the third party or parties."[46] The silence of the Directive with regard to the legitimate interest of the data subject or controller as a criterion for the assessment of the level of data protection can be seen as a contradiction to the general principles rendering data processing legitimate.

C. Comparison of the Level of Protection

1. *Definition of the Level of Protection*

The second part of the two-fold test[47] assessing the adequate level of protection involves a comparison of the level of protection between the two countries. A level of protection needs to be established in order to compare it with the level of protection of the third country. Two possibilities for the establishment of the level of protection are crucial: (1) the

45. Directive 95/46/EC art. 17(1).
46. Directive 95/46/EC art. 7(f).
47. *See supra* § IV. (B)(1).

level of protection of the individual European Member State from which the data will be transferred;[48] or (2) the level of protection arising from the Directive.[49] The Directive is silent on which approach should be followed.

2. *Level of Protection of the Member State*

The level of protection of the Member State could be the key point. Arising from the legal nature of the Directive, the Member States are obliged to implement the Directive: it "shall be binding, as to the results to be achieved, upon each Member State to which it is addressed, but shall leave to the national authority the choice of form and methods."[50] According to the Directive, the Member States shall "determine more precisely the conditions under which the processing of personal data is lawful."[51] The wording shows that it is up to the Member States to set the conditions of a lawful processing of personal data. The Directive marks the beginning and not the completion of the harmonization in the field of the data protection law.[52]

Also, the Directive states that "Member States will be left a margin for manoeuvre, which may, in the context of the implementation of the Directive, also be exercised by the business and social partners."[53] The Directive contains several legal terms, which could be implemented in different ways. The Member States have been allowed a wide margin for discretion. Therefore, the national data protection laws can differ from each other in a significant way. In practice, for example, the obligation to notify the supervisory authority before carrying out any automatic processing operation[54] is regulated quite differently in the Member States.

3. *Level of Protection of the Directive*

A different approach would be to look at the Directive's level of protection. The Directive itself indicates that a European-wide level could be the relevant factor. It is stated that the "Member States and the Commission shall inform each other of cases where they consider that a third party does not ensure an adequate level of protection."[55] So, there is a

48. *See* Spiros Simitis, *Die EU-Datenschutzrichtlinie - Stillstand oder Anreiz?*, Neue Juristische Wochenschrift 281, 285 (1997); Hans H. Wohlgemuth, *Auswirkungen der EG-Datenschutzrichtlinie auf den Arbeitnehmer-Datenschutz*, Betriebs-Berater 690, 694 (1996).

49. *See* Ellger, *supra* n. 43, at 8.

50. Art. 249(3) of the Treaty establishing the European Community.

51. Directive 95/46/EC art. 5.

52. Dammann, *supra* n. 31, at 133.

53. Directive 95/46/EC Recital (9).

54. Directive 95/46/EC art. 18(1).

55. Directive 95/46/EC art. 25(3).

flavor of a European-wide approach so that the conclusion could be drawn that the Directive's level of protection is crucial.

4. *Criticism*

First of all, it is not satisfactory that the Directive does not explicitly state whether the Directive's or the relevant Member State's level of protection is the relevant factor. There are some provisions, which could be interpreted as a solution for the open point. However, it is desirable for reasons of legal certainty that the Directive clearly states which level of protection has to be followed.

From my point of view, the Directive's level of protection should be the relevant factor. As discussed above, the Member States have a wide margin of discretion when implementing the provisions of the Directive. Member States could set down a minimum or maximum standard in their national laws. Possibly, there is also a wide difference between the national data protection laws. It would be unjust to have different factors for the comparison. In practice, there could be different requirements for the data transfer depending from which Member State the data will be transferred. Especially international companies can evade national laws with a high standard of data protection by choosing- for the export of data - a Member State with a lower standard.

D. The Directive's Level of Protection

1. *Structure of the Directive*

The Directive should be the basis for the comparison of the level of protection. Every provision would be part of the process of comparison. Therefore, it could be arguable to use the structure as the foundation of the assessment:

- Chapter I: General Provisions;
- Chapter II: General Rules on the Lawfulness;
- Chapter III: Judicial Remedies, Liability and Sanctions;
- Chapter IV: Transfer of Personal Data to Third Countries;
- Chapter V: Code of Conduct;
- Chapter VI: Supervisory Authority; and
- Chapter VII: Community Implementing Measures.

2. *Approach of the Working Party*

"A Working Party on the Protection of Individuals with regard to the processing of Personal Data" ("working party") was set up and it "shall have advisory status and act independently."[56] The working party is

56. Directive 95/46/EC art. 29(1); *see* Heil, *Die Artikel 29-Datenschutzgruppe*, Datenschutz und Datensicherheit 471 (1999).

composed of representatives of the supervisory authority, which each Member State is required to establish. These supervisory authorities have the task of monitoring the application of the national data protection laws.[57] The working party has submitted a report on the question of what is meant by "adequate level."[58] In the report, the working party proposes to look on the content of the rules applied and also on the enforcement procedure. The report sets out the basic principles as being:

- the purpose limitation principle;
- the data quality and proportionality principle;
- the transparency principle;
- the security principle;
- the right of access, rectification and opposition principle; and
- the restrictions on onward transfer principle.[59]

These principles are in line with the European Union's internal requirements.[60] However, the report adds special rules in the field of sensitive data, direct marketing and automated decision-making. The report also makes clear that there must be a good level of compliance in order to approve the adequate level of data protection. However, the report does not require that an omnibus data protection law be in place. It recognizes that self-regulations could also ensure adequate protection. Also, the working party recognizes that Member States should look at the circumstances of each case by saying

> A positive finding should not in principle be limited to countries having horizontal data protection laws, but should also cover specific factors within countries where data protection is adequate, even though in other sectors the same country's protection may be less than adequate.

The report goes on to consider supervisory authorities and the manner in which they may deal with cases of inadequacy. Also, it proposes that European-wide contractual arrangements might be developed in order to deal with such cases.[61]

V. CRITICISM AND OWN APPROACH

A. General

The structure of the Directive does not really help, in that it does not reflect the Directive's aim of data protection. It could be regarded as a

57. *See* Kees Jan Kuilwijk, *Recent Developments in E.U. Privacy Protection Regulation*, 6 Intl. Trade L. & Reg. 200, 201 (2000).

58. Working party established by Article 29 of Directive 95/46/EC, preparation of a methodology for evaluating the adequacy of the level of individuals with regard to the processing of personal data, GD XV D/5025/98 of 24 July 1998.

59. Aldhouse, *supra* n. 23, at 77; Blume, *supra* n. 18, at 69.

60. Shaffer, *supra* n. 6, at 419.

61. Aldhouse, *supra* n. 23, at 77.

basis for an assessment, but does not support any substantial test measure.

The approach of the working party does not seem to be conclusive. Certainly, useful principles are stated. However, procedural provisions have gained an importance, which is not reflected by the Directive. Especially, the criterion of "the right of access, rectification and opposition" has less practical influence in the European Union. Regardless of this fact, it is stated as one of the main principles.

The basis for the comparison of the adequate level should be the objective of the Directive. The objective of the Directive is that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[62] The conclusion can be drawn that the art and manner of the protection of the "fundamental rights and freedoms of natural persons" and of the "right to privacy" are essential.

With regard to the overwhelming objective of the Directive, in my opinion, the criteria should be as follows:

- lawfulness of the processing of personal data;
- special protection of sensitive data;
- rights of the data subjects;
- security of processing; and
- control and enforcement measures.

The criteria are mentioned in the Directive, and they ensure that the objective of the Directive as stated above is secured. It has to be reviewed whether and how they are regulated in the data protection laws of the country to whom the data are transferred. However, the following sections will explain each criterion in detail.

B. Lawfulness of the Processing of Personal Data

First of all, we need to have "personal data." According to the definition stated in the Directive, "personal data shall mean any information relating to an identified or identifiable person."[63] The definition appears broad and will extend to images and other non-textual information. Recital 14 of the Directive makes it clear that the processing of sound and image data is to be covered by the Directive.[64]

The data subject must be identifiable. Elements of such an identification can be the "identification number" and/or with reference to the "physical, physiological, mental, economic, cultural or social identity."[65]

62. Directive 95/46/EC art. 1(1).
63. Directive 95/46/EC art. 2(a).
64. Bainbridge, *supra* n. 14, at 19.
65. Directive 95/46/EC art. 2(a).

However, the list is not exclusive, and additional elements can be crucial for the identification.

The Directive forbids any processing of data if one of the provisions for the lawfulness of the processing is not met. According to the Directive, personal data may be processed only if:

a) the data subject has unambiguously given his consent; or
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) processing is necessary in order to protect the vital interests of the data subject; or
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) processing is necessary for the purpose of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).[66]

The mentioned conditions are alternatives. For a particular processing operation, there only needs to be compliance with one of these conditions. In the vast majority of the cases, it is sufficient to rely on the conditions in (b) to (f) so that consent is not required.[67] The consent as such could be problematic. In connection with a data transfer, it will be doubtful whether the data subject can be informed in a sufficient manner so that he is able to fully understand the consequences of consent.[68] Also, consent has the disadvantage that it can be revoked.[69] Apart from that, the Directive is silent on whether a once and for all assent will suffice or whether the data subject has to be asked periodically.[70]

As stated above, it is difficult to envisage a situation where one of the conditions in (b) to (f) does not apply. All of these alternatives to seeking and receiving the consent are expressed as being "necessary." However, the expression will not be interpreted in a strong sense.[71]

In addition to the mentioned provisions whereby processing would be lawful, the Directive sets down principles relating to data quality. One of these principles is that the handling of data should relate to a

66. Directive 95/46/EC art. 7.
67. Bainbridge, *supra* n. 14, at 24.
68. Blume, *supra* n. 18, at 71.
69. Christopher Kuner, *EU Regulations Threaten International Data Flows*, Intl. Tech. L.R. 39, 40 (2001).
70. Bainbridge, *supra* n. 7, at 63.
71. Bainbridge, *supra* n. 7, at 54.

certain purpose. Therefore, the Directive states that Member States shall provide that personal data must be:

a) processed fairly and lawfully;
b) collected for specified explicit and legitimate purpose and not further processed in a way incompatible with those purposes . . .; and
c) adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed.[72]

Fair and lawful processing means that the individual may not be deceived or misled about the purpose for which the data are processed and must be provided with certain information such as the identity of the data controller. Processing for a certain purpose has the meaning that the data controller must state the purpose for which it is obtaining personal data and may not take any actions which are incompatible with such a purpose. The third principle is the adequacy of data. The processed data must be adequate, relevant, and not excessive in relation to the purpose for which they are collected.[73]

With regard to the comparison of the level of data protection, the question must be asked whether the data protection law of the recipient country does provide for regulations similar to the mentioned principles.

C. Special Protection of Sensitive Data

Data, and especially sensitive data, can infringe the fundamental rights, and in particular the right to privacy of natural persons. Therefore, sensitive data require a higher level of data protection. The Directive provides that "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical belief, trade-union membership, and the processing of data concerning health or sex life."[74] There are some exceptions to this prohibition, i.e. where:

a) the data subject has given his explicit consent;
b) processing is necessary for the purpose of carrying out obligations in the field of employment law;
c) processing is necessary to protect the vital interest of the data subject or another where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade union aim in condition that the processing relates solely to the member of the body or persons having regular contact in connection

72. Directive 95/46/EC art. 6.
73. Overstraeten, *supra* n. 11, at 59.
74. Directive 95/46/EC art. 8(1).

with its purposes and the data are not disclosed to a third party with the consent of the data subjects; and

e) processing relates to data, which are manifestly made public by the data subject, or is necessary for the establishment, exercise or defence of legal claims.[75]

The requirements for a valid consent as stated in (a) are strict: such a statement must be freely given, specific and informed.[76] An example of (b) would be where an employer is required by law to make official returns, say specifying the number of disabled persons working for him. Exception (c) could be relevant in cases where the data subject is unconscious and in need of a blood transfusion. Whilst (d) and the first part of (e) are self-explanatory, the second part of (e) could play a major role in the course of a discovery procedure.[77]

Apart from that, an exception is stated for processing of data required for lawful medical purposes.[78] Also, the processing of data for reasons of substantial public interests and of revealing criminal offences are exempted.[79] Recital 34 indicates what might be covered by this public interest: processing for purposes in connection with public and social protection, especially in order to ensure the quality and cost-effectiveness of the procedures settling claims for benefits and services in the health insurance system, scientific research and government statistics.[80]

The description of what can amount to sensitive data in Art. 8(1) of the Directive appears to be exhaustive. But it cannot be so as data relating to offences are included. The acid test can be deduced from Recital 33 whereby data, which are capable by their nature of infringing fundamental freedoms or privacy, should not be processed. Clearly, this can include criminal convictions. However, it should be noted that, in most cases, this information is publicly available anyway.[81]

It may be difficult to describe the criteria of fields, which need a special protection in legal terms. However, it is clear that a processing of data carrying a certain degree of sensitivity needs to have special conditions. Therefore, the art and manner in which the processing of sensitive data is regulated have to be assessed in connection with the comparison of the level of data protection. The data protection law in question should have safeguards that are at least comparable with the Directive.

---

75. Directive 95/46/EC art. 8(2).

76. Dag Weise Schartum, *Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects*, 15 Intl. Rev. L., Computers & Tech. 157, 163 (2001).

77. Bainbridge, *supra* n. 14, at 25.

78. Directive 95/46/EC art. 8(3).

79. Directive 95/46/EC art. 8(4) and (5).

80. Bainbridge, *supra* n. 14, at 25.

81. Bainbridge, *supra* n. 7, at 57.

D. Rights of the Data Subjects

Data subjects have several rights under the Directive: the right to access to data and to object. The right of access is stated as follows:

> Member States shall guarantee every right to obtain from the controller: a) without constraint at reasonable intervals and without excessive delay or expense conformation as to whether or not data relating to him are processed . . ., communication to him in an intelligible form of the data undergoing processing . . ., knowledge of the logic involved in any automatic processing of data concerning him . . ., b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive.[82]

It does not seem that the provision places a positive duty on data users to keep a record of disclosures. However, it is good practice to keep comprehensive records of processing.[83]

The data subject also has the right - at least in cases referred to in Art. 7(e) and (f) of the Directive[84] - to object on compelling legitimate grounds to the processing of data relating to him. In case of a justified objection, the processing may no longer involve those data.[85] The right to object is related to the particular situation of the data subject, especially in cases where the lawfulness of the processing of data is not so clear, and is often subject to interpretation. The data subject does not have a blanket right to prevent the processing of his data under any circumstances. The rights to object are not as extensive as that.[86] The Directive does not decide the complex question whether the data subject is owner of his data, but it makes clear that they may not be processed if an infringement of privacy takes place.[87] Without having the right to object, an infringement of the data subject's right to privacy may easily be infringed. Therefore, these rights have to be taken into account in any comparison of the level of data protection.

E. Security of Processing

Any data protection law, which does not provide for security measures, would be less effective. The Directive states that the "controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access."[88] The controller is obliged to take measures commensurate with the risks represented

82. Directive 95/46/EC art. 12.
83. Bainbridge, *supra* n. 14, at 34.
84. *See supra* § V.(B).
85. Directive 95/46/EC art. 14(a).
86. Bainbridge, *supra* n. 7, at 64.
87. Blume, *supra* n. 18, at 67.
88. Directive 95/46/EC art. 17(1).

by processing and the nature of the data taking into account the state of art and the cost of implementation. A balance is to be struck between the seriousness of the consequences of a failure and the costs involved.[89] The data controller's duties extend to ensuring the reliability of those employees who have access to personal data.[90]

In this respect, security objectives play an important part: they are high-level goals for an organization. The standard on security for communication networks state the following objectives:

- accountability, that legitimate users shall be accountable for the utilisation of any services;
- integrity, that the system behaves in an expected way, and that the information stored or exchanged is correct;
- confidentiality, that information exchanged shall be kept confidential when needed, and that access to information shall be controlled and limited to those with a legitimate right,
- availability, that information shall be available to authorised users.[91]

The objectives have to be taken into account assessing the security measures of the recipient country. Apart from that, there are three categories of security measures:

- physical like infrastructures supporting security;
- logical like cryptographic protection, authentication and access control;
- administrative like national security policy and legislation.[92]

The objectives and the security measures have to be taken into account when assessing the status of the security of processing of the recipient country. The above-mentioned guidelines are relevant for the assessment.

F. Control and Enforcement Measures

Control and enforcement measures play an important part in the effectiveness of any data protection law. Without these measures, any data protection law would be "a tiger without teeth." According to the Directive, a data subject has the right to judicial remedies for any breach of the rights guaranteed to him.[93] Also, the data subject can claim damages for any unlawful processing operation.[94]

---

89. Bainbridge, *supra* n. 14, at 26.

90. Overstraeten, *supra* n. 11, at 60.

91. Dave Newman & Sathya Rao, *Regulatory Aspects of Privacy and Security - A View from the Advanced Commincations Technologies and Services Programme*, 9 Info. & Communs. Tech. L. 161, 162 (2000).

92. *Id.*

93. Directive 95/46/EC art. 22.

94. Directive 95/46/EC art. 23(1).

Apart from that, supervisory authorities may ensure that data protection laws are followed. The Directive states that Member States shall establish public authorities, which shall be responsible for monitoring the application of the relevant data protection law. Each authority shall be endowed with investigative powers; effective powers of intervention and the power to engage in legal proceedings.[95] For the assessment of the adequate level of data protection, the data protection law of the recipient country should provide at least for control and enforcement measures similar to the Directive. Lately, the data protection authorities of the Member States have shown an increased willingness to impose sanctions in case of violations of data transfer restrictions.[96]

VI. SUMMARY

The Directive does not state whether the Directive's or the relevant Member State's level of protection is the relevant factor. In my opinion, the Directive's level of protection should be crucial. The Directive's objective needs to be taken into account in order to establish the criteria for the determination of the adequate level of protection. Considering the objective of the Directive, the criteria for the comparison should include: lawfulness of the processing of personal data; special protection of sensitive data; rights of the data subjects; security of processing; control and enforcement measures. All these criteria are set forth in the Directive, and they ensure that the objective of the Directive is achieved.

95. Directive 95/46/EC art. 28(1), (3).

96. Kuner, *supra* n. 69, at 39.