UIC John Marshall Journal of Information Technology & Privacy Law

Volume 14
Issue 3 *Journal of Computer & Information Law - Spring 1996*

Article 1

Spring 1996

Harmonisation of European Union Privacy Law, 14 J. Marshall J. Computer & Info. L. 411 (1996)

Ulrich U. Wuermeling

HARMONISATION OF EUROPEAN UNION PRIVACY LAW

by ULRICH U. WUERMELING†

CONTENTS

† 1992 law degree, Staatsexamen, Bayreuth, Germany; 1993 Master of International Business Law, LL.M., London; 1993-1996 assistant researcher at the University of Würzburg, Germany; currently attorney-at-law in Frankfurt, Germany, and co-editor of the German privacy journal "Datenschutz-Berater."

I. INTRODUCTION

On July 24, 1995, the Council of the European Union finally reached a decision regarding a Data Protection Directive ("Directive").[1] The Directive represents a single step in the world-wide development of data protection regulations attempting to protect individual privacy rights

1. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Council Directive].

and freedoms in view of the rapid advance of new technology.[2] This article examines present national and international regulations in comparison with the Directive in order to analyze the potential practical impacts.

The first part of this article provides a historical background and an introduction to national and international initiatives for data protection regulation. Starting from principles of privacy, early national regulations are reviewed. To put the Directive into perspective, other important international initiatives in the field of data protection, including their basic ideas, historical background, and effect are examined. The third part of the article chronicles the history of the European Directive. The European Parliament made several attempts before the Commission introduced the First Proposal for a Directive in 1990.[3] This section reviews the decision-making process and parties involved in the general discussion about the Directive.

The fourth part of this article examines in detail the provisions of the Directive. It interprets and compares all of the proposed regulations with those of the OECD, the UN and Council of Europe. The article also discuses the impact of the Directive on the national data protection laws in Europe. Because the Directive is not limited to transborder data flow provisions, but covers the entire range of data protection regulations, the Member States' laws required significant changes.

The Directive integrates several systems into a single consistent regulation. Present national and international regulations, as well as recommendations and amendments from the European Parliament, Member State governments, trade associations, data protection commissioners, and others have influenced the Directive and contributed to the final compromise. This article traces the origin of the various provisions in the Directive from their original proposed form to aid in their interpretation.

Where a common interpretation is not possible, this article describes the possible range of interpretations, particularly from the German and U.K., perspectives. Unlike the U.K., German data protection law is strongly based on the German Constitution. This results in significant differences in interpreting the provisions. Based on this analysis, this

2. Nineteen European countries and countries like Japan and Canada passed Data Protection Acts. Other countries like the United States passed some legislation covering privacy; for an example of U.S. legislation, *see* Robert Bigelow, *Privacy*, 2 COMP. LAW SER. REP 50 (1993); Ronald J. Krotoszynski, *Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law*, 1990 DUKE L.J. 1398, 1434 (1990); Joel R. Reidenberg, *The Privacy Obstacle Course Hurdling Barriers to Transactional Financial Services*, 60 FORDHAM L. REV. S137 (1992).

3. Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3 [hereinafter First Proposal].

article considers whether the Directive can achieve its intended goal of harmonising data protection standards in Europe.

II. HISTORICAL BACKGROUNDS

A. Basic Foundations

Data protection initiatives were triggered by the development of new technology for data processing in the second half of this century. However, data protection is only one part of the broader and older issue of "privacy." Based on the idea of privacy as a part of freedom rights, data protection regulations are structured to fit into three different categories:

1. The first basis for data protection initiatives is the right of privacy which was identified by Justice Brandeis in 1928 as "the right to be let alone."[4] In the modern information society, the right to be let alone includes the right to control any communication related to a person. The subject should have the freedom to decide the extent to which he takes part in society and the extent to which he remains separated from it. The right to be let alone finds its limit in the need for the community in society. There must be a balance between the right to be let alone and the legitimate interests of a society. Therefore, all data protection regulations provide exemptions from the principle that the subject has to give consent to processing of data about the subject person. The extent of these exemptions is one of the important indicators for the character of a data protection regulation.

2. If there is a need to provide rights for society to process information without the subject's consent, the second basic idea of data protection regulations, the "right to know," comes into play. The right to know is directly connected to the right to be let alone, because the subject has the right to decide where the line between the private and the open part of his own personality is drawn. The principle of self-determination provides the possibility to build up one's own personality in such a way that the subject has to know about the information other people already have about him. There is also a legitimate interest of the subject to know because of the possibility that data about him could be wrong and have to be corrected. All data protection regulations grant the subject, to some extent, a right to obtain information about the processing of personal data. A registration system is also part of the right to know, because it helps the subject find out about processing of his personal data. A similar effect is caused by specific legal permissions for processing. However, the right to know is limited in view of the needs of the society.

---

4. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see* Matthew N. Kleiman, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 Nw. U. L. Rev. 1169, 1173 (Summer 1992).

3. The third basic block of data protection regulations is about "measures to secure" the practical effect of data protection rights. Supervisory authorities, registration procedures, remedies, liability and sanctions are provided to enforce data protection regulations.

B. First Data Protection Laws

In the late 1960s, the government of the German Land of Hesse planned to push the use of information technology in the public sector.[5] The idea was to provide information technology for all parts of Hesse to support similar living standards in the countryside and the capitals. In implementing this concept, the government realised that such a system would cause a huge collection of private data and therefore create a dangerous power in the hand of the government. These concerns led to the first data protection legislation in the world. Hesse passed its Data Protection Act in 1970. Sweden followed in 1973 with the first national Data Protection Law. Data protection legislation was then passed in several countries.[6] However, several European Union countries, including Greece and Italy, do not yet have a general data protection legislation.

C. Activities of International Organizations

One of the advantages of information technology is that data can be transmitted electronically over unlimited distances. Therefore, every legal problem connected to information technology becomes an international issue. International organizations have taken different actions to harmonize information technology law. Quickly they recognized that data protection was of paramount importance.

1. *Organisation for Economic Cooperation and Development*

The Organisation for Economic Cooperation and Development ("OECD") started to look at problems of data protection law in the 1970s.[7] In 1978, the OECD founded an "Expert Group on Transborder Data Barriers."[8] The Group worked on international regulations for transborder data exchange. Data protection was one of the issues in this field. The OECD decided to support an international regulation and the

---

5. *Hessische Zentrale für Datenverarbeitung*, Grosser Hessenplan 1970.

6. See Spiros Simitis et al., Kommentar zum Bundesdatenschutzgesetz § 1 at 108 (1992).

7. The first work in this field was done at an OECD Seminar held in 1974. *See* Organisation for Economic Cooperation and Development, *Policy Issues in Data Protection and Privacy*, *in* 10 OECD Informatics Studies (1974).

8. Gassmann, The Activities of the OECD in the Field of Transnational Data Regulation in Online, Data Regulation and Third World Realties 177, 182 (1978).

Council of the OECD passed Guidelines[9] in the form of a Recommendation on September 23, 1980. The Guidelines have been endorsed by all OECD Member States.

The OECD regulation covers some of the basic principles of data protection law. These principles are the:

- collection limitation principle,
- data quality principle,
- purpose specification principle,
- use limitation principle,
- security safeguard principle,
- openness principle, and
- individual participation principle.

The underlying aim for the activities of the OECD was not to protect individual privacy interests.[10] The OECD saw the national data protection laws as protectionist regulations and non-tariff trade barriers.[11] In order to overcome these barriers, the Expert Group worked on guidelines for the regulation of data protection. The seven principles of the OECD Guidelines show quite a strong approach. However, the regulations of the Guidelines give Member States easy opportunities to limit their effect. Section 3(a) of the Guidelines provides that the principles should be interpreted in view of the individual risk of the data processing. Section 4 provides a general possibility to regulate exemptions. In this respect, the OECD Guidelines seem to be a free data flow regulation rather than a data protection regulation.[12] Section 16 of the Guidelines states that all reasonable steps should be taken by Member States to ensure that transborder flows of personal data, including transmissions through a Member State, are uninterrupted and secure. It is clear that in view of this idea, the data protection principles of the OECD Guideline only represent a minimum standard of data protection.

The legal effect of the OECD Guidelines was limited because of three additional reasons: first, the OECD members (24 nations) do not have a legal duty to implement the OECD regulations.[13] Second, the extent of wide exemptions in the OECD Guidelines limits its effect. Third, the Council of Europe took action in the field of data protection regulation by

9. ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data, in* 80 OECD DOCUMENT C 58 (final 1980) [hereinafter *OECD Guidelines*].

10. Von Richter am VG Hans-Hermann Schild, *Datenschutz in Europa*, 24 EUZW 745, 747 (1991).

11. SIMITIS, *supra* note 6, § 1 at 143.

12. *Id.* ADRIANA C.M. NUGTER, TRANSBORDER FLOW of PERSONAL DATA WITHIN THE EC 22 (Deventer 1990).

13. Reinhard Ellger, *Datenexport in Drittstaaten*, 1 CR 2 (1993); Peter Blume, *An EEC Policy for Data Protection*, 11 COMPUTER/L.J. 399, 405 (1992).

passing the Council of Europe ("CoE") Convention on Data Protection.[14] Several countries are members of both organizations. It will be seen in the following section that the regulations in the CoE Convention are stronger than those of the OECD Guidelines. Therefore, member states of both organizations had to follow the CoE Convention rather than the OECD Guidelines.

2. *Council of Europe*

The Council of Europe first focused on the problems of personal data in 1968 as a result of a Parliament Assembly recommendation.[15] The CoE asked the Committee of Ministers to verify whether and to what extent the regulations in the Human Rights Convention and the law of the Member States were able to protect individuals from the risks of new technologies.[16]

For the Council of Europe, data protection was a question of human rights. That was the main difference from the OECD initiative. The fundamental idea of the Council of Europe is to protect privacy rather than to prevent transborder data barriers. Data protection was seen as a part of the personal privacy rights in the sense of Article 8(1) of the Human Rights Convention.[17]

In 1973, the Committee of Ministers passed the first recommendation on data protection for the private sector and, in 1974, the public sector.[18] However, the Council realised that the problem could not be solved with the weak legal instrument of a recommendation. In 1976, the Committee of Ministers instructed an expert group to prepare a draft version of a Convention on data protection.[19] A second expert group prepared the final version in 1980. On January 28, 1981 the CoE Convention[20] was opened for signature.

The CoE Convention Chapter II regulates the basic principles of data protection. The following subjects are covered:

- duties of the parties (Article 4),
- quality of data (Article 5),
- special categories of data (Article 6),
- data security (Article 7),

14. *Council of Europe*, Convention (No. 108) for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series No. 108 (Jan. 1981).

15. *Council of Europe*, Parliamentary Assembly Recommendation 509 (1968).

16. *See* SIMITIS, *supra* note 6, § 1 at 120.

17. *Council of Europe*, Convention for the Protection of Human Rights and Fundamental Freedoms [hereinafter Convention] (1950).

18. Recommendations (73)22 and (74)29; *see* SIMITIS, *supra* note 6, § 1 at 120.

19. *See* NUGTER, *supra* note 12, at 25.

20. *Council of Europe*, *supra* note 15.

- additional safeguards for the data subject (Article 8),
- exemptions and restrictions (Article 9),
- sanctions and remedies (Article 10), and
- extended protection (Article 11).

While the CoE Convention came into force on October 1, 1985, it has no direct legal effect on the law or jurisdiction of the Member States,[21] because it is a "non self-executing treaty."[22]

3. *United Nations*

The United Nations was one of the first intermediate organizations to examine the rising problems of electronic data processing and human rights. On December 19, 1968 the General Assembly of the United Nations asked the General Secretary to order a survey about the effects of technical progress on human rights.[23] A draft report was presented to the General Assembly in 1970[24] and a second resolution was passed to show the preference of the General Assembly to do further work on the subject.[25] Then, the General Assembly requested the Human Rights Commission to prepare regulations to secure human rights in view of new technological developments.[26] In 1985, commission member Louis Joinet submitted a first draft version[27] and in 1988 he submitted a second draft.[28] In December, 1989, the General Assembly of the Commission on Human Rights of the United Nations adopted the UN Resolution for the regulation of computerized personal data files.[29] The principles of the UN Resolution are very similar to those of the CoE Convention, but have no direct legal effect on the Member States.

---

21. NUGTER, *supra* note 12, at 26.

22. *See* SIMITIS, *supra* note 6, § 1 at 122. "Non self-executing" means that each Member State must enact enabling legislation for the CoE Convention to become effective.

23. G.A. Res. 2450, U.N. GAOR, 23d Sess. (1968); *see* SIMITIS, *supra* note 6, § 1 at 148.

24. *Report of the Secretary General on Human Rights and Scientific and Technological Developments*, U.N. Commission on Human Rights, 26th Sess., Provisional Agenda Item 18, U.N. Doc. E/CN.4/1028 (Feb. 26, 1970).

25. G.A. Res. 10, U.N. GAOR 28th Sess. (1973).

26. G.A. Res. 3026, U.N. GAOR 27th Sess., pt. B (1972).

27. *Draft Guidelines for the Regulation of Computerised Personal Data Files, Report submitted by Mr. Louis Joinet*, U.N. Commission on Human Rights, 38th Sess., Provisional Agenda Item 10, U.N. Doc. E/CN.4/Sub.2/1985/21 (June 23, 1985).

28. Louis Joinet, *Final Report of the Special Reporter on the Guidelines for the Regulation of Computerized Personal Data Files*, U.N. Economic and Social Council, Commission of Human Rights, Subcommission on Prevention of Discrimination and Protection of Minorities, 40th Sess., Provisional Agenda Item 11, U.N. Doc. E/CN 4/Sub. 2/22 (1988).

29. *Guidelines for the Regulation of Computerized Personal Data Files, Final report submitted by Mr. Louis Joinet*, U.N. Commission on Human Rights, 40th Sess., Provisional Agenda Item 11, U.N. Doc. E/CN.4/Sub.2/1988/22 (July 21, 1988) [hereinafter *Guidelines*].

III. THE DEVELOPMENT

A. History of the European Initiatives

The European Parliament first focused on the issue of data protection in 1974[30] and passed two Resolutions in 1975[31] and 1976.[32] In May, 1979, the European Parliament adopted the third Resolution on data protection[33] which included data protection principles. The Parliament called the Commission "to prepare a proposal for a directive on the harmonisation of legislation on data protection to provide citizens of the Community with the maximum protection."[34] However, a resolution itself has no direct binding force and the Commission did not prepare a directive at this stage.

On July 29, 1981, the Commission recommended that Member States ratify the CoE Convention before the end of 1982.[35] But, the Commission also reserved the right to propose that the Council should adopt an instrument on the basis of the EC Treaty.[36] The Parliament acted again in 1982 in the field of data protection.[37] The initiative was based on a report of the Legal Affairs Committee.[38] The report stated that a Community directive was "as urgently needed as ever before to provide the highest possible level of protection."[39] However, the Commission produced regulations for the common market in the field of information technology without any activity to ensure the protection for the processing of personal data.[40] Further, the Commission repeated its viewpoint that the Member States should sign and ratify the CoE Con-

30. *See* Nugter, *supra* note 12, at 29.

31. *Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, Eur. Parl., 1975 O.J. (C 60) 48.

32. *Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*, Eur. Parl., 1976 O.J. (C 100) 27.

33. *Resolution on the Protection of the Rights of the Individual in Connection in the Face of Technical Developments in Data Processing*, Eur. Parl., 1979 O.J. (C 140) 34.

34. Nugter, *supra* note 12, at 30.

35. Commission Recommendation Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 81/679/EEC, 1981 O.J. (L 246) 31 [hereinafter Commission Recommendation].

36. *Id.*

37. *Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing*, Eur. Parl., 1982 O.J. (C 87) 39 [hereinafter *Resolution on Protection*].

38. *Sieglerschmidt Report for the Legal Affairs Committee*, Eur. Parl. Doc. (1-548) 81 [hereinafter *Sieglerschmidt Report*]; *see also* Nugter, *supra* note 12, at 30.

39. *Sieglerschmidt Report*, *supra* note 38 at 34.

40. Simitis, *supra* note 6, § 1 at 143; Spiros Simitis, 1 RDV 3, 7 (1990); Riegel, 4 ZRP 132, 133 (1990).

vention in order to solve the need of data protection regulations.[41]

In 1990, three years before the proposed European Single Market was completed, five Member States of the European Community had still not ratified the CoE Convention.[42] As a result, the Commission changed its opinion and in 1990 published the First Proposal for a Data Protection Directive.[43]

B. Six Initiatives

To ensure data protection in Europe, the First Proposal was published together with five other initiatives. One of these initiatives was a draft for a Resolution of the Representatives of the Governments of Member States. The effect of the Resolution was that the Member States had to use the same protection principles set out in the Directive for the public sector. However, the legislative power of the Community does not allow it to regulate the public sector in a field which is not governed by community law.[44] Therefore, the Commission asked the Member States to confirm the Resolution.[45] One of the reasons for the Resolution is that it would be difficult to make separate regulations for the public sector. The distinction whether or not a collection of personal data is prepared under community related law would be difficult. Community law becomes part of the Member States' law only if it is introduced by ratification of community directives. Commissioner Martin Bangemann pointed out that the question of power to regulate the different sectors of public law should not be discussed. He argued that a clear scope of the European regulation is needed in order to remove barriers to the flow of personal data.[46]

Although one of the six initiatives dealt with the application of the Directive to the institutions of the Community,[47] the institutions have no general regulations regarding data protection yet. The Decision, therefore, intended to enforce the Directive for the Community administration. In order to comply with the Directive, the Community will have

41. Nugter, *supra* note 12, at 31.

42. The five countries include: Belgium, Greece, Italy, Portugal, and Spain.

43. First Proposal, *supra* note 3, at 3.

44. The German board of the federal states claimed that the First Proposal for a Data Protection Directive granted insufficient powers especially in the public sector. *See Mitteilung der Kommission der Europäischen Gemeinschaften zum Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und zur Sicherheit der Informationssysteme*, 690 Bundesrat BRD 1 (Dec. 14, 1990).

45. Draft Resolution of the Representatives of the Governments of Member States of the European Community Meeting within the Council, COM(90)314.

46. Martin Bangemann, *Datenschutz — so wichtig wie Umweltschutz*, EG-Magazin, October, 1990, at 10, 11.

47. Commission Declaration on the Application to the Institutions and Other Bodies of the European Communities of the Principle Contained in the Council, COM(90)314.

to name a European data protection commissioner. He would be responsible for the administrative work of the Community but not for the Member States.

Another initiative provided specifically for data protection in the digital telecommunication market ("ISDN"). The fifth initiative deals with the question of whether the Community as such should sign the CoE Convention. The last initiative sets out a two year action plan to prepare common regulations for information security.

The First Proposal was sufficiently detailed to ensure a similar level of protection in the Member States. It was based on three main data protection ideas which can also be found in the OECD Guidelines, the CoE Convention and the UN-Guidelines. These basic ideas are the limitation of processing, openness, and security safeguards. In some provisions, the Proposal gave the possibility for individual national regulations.[48] However, compared with the CoE Convention and the OECD Guidelines, the First Proposal was stronger and much more detailed. The experiences with the CoE Convention showed the Commission that a general regulation would not be able to accomplish the intended effect. Thus, the Commission wanted a detailed regulation in order to unify data protection laws on a high level.[49]

By introducing the Directive on ISDN as one of the initiatives, the Commission showed its intention to provide sectorial data protection regulations in the future.[50] In addition, Article 30 of the First Proposal proposes a rule giving the Commission the power to introduce specific regulations. The need for such regulations is clear because some Member States, like Germany, already have sectorial regulation in the field of labour law, social security law and other fields. Differences in those regulations can cause problems similar to differences in the general standard of the data protection law. However, the move towards more "solidarity" in the European Union will affect the power of the Commission to regulate specific sectors. The summit of Edinburgh in 1992, for example, was especially forceful in making the Commission concentrate on general subjects.[51]

C. Decision-Making Process

The Commission had the power to create the Directive based on Article 100a of the EC-Treaty. Therefore, the decision about the Directive

48. *See* Articles 6(3)2, 8(3), 21(2), and 23 of the First Proposal, *supra* note 3; *see* Simitis, *supra* note 6, § 1 at 154.

49. Bangemann, *supra* note 46, at 11.

50. Simitis, *supra* note 6, § 1 at 127.

51. *See* Kommission der Europaishen Gemeinschaften, *Europaischer rat Edinburgh*, 15 EG-Nachrichten, Dec. 21, 1992, at 14.

was to be made under the procedure of Article 189(b) of the EC Treaty. The regulation is called the "co-operation procedure" and was introduced in 1986.[52] It was amended by the Maastricht Treaty in 1993 in order to give more power to the Parliament.

The decision-making process has two main parts; the first one leads to the common position and the second one to the final directive. The first part starts with a proposal for the directive. Sometimes the Commission issues a green book beforehand, however, in the case of the Data Protection Directive, the Commission started directly with the First Proposal. In 1990, the Commission handed over the proposal to the Council, the Parliament, and the Economic and Social Committee for their recommendations. During this time, a group of Member State specialists was set up to discuss the Directive and to give advice to the Council.[53] The Economic and Social Committee[54] and the Parliament[55] gave their recommendations on the First Proposal in 1991 and 1992.

Based on the general discussion, the Commission prepared the Second Proposal nearly two years after the first. The legal procedure of the decision-making process for a Directive necessitates that the Commission take into account the recommendations of the Parliament.[56] However, the Commission tried to find a conclusion for all parties involved. Therefore, the Second Proposal was not influenced by the Parliament recommendations. The Working Party on Economic Questions ("Data Protection") also played an important role in the revising procedure. The Second Proposal[57] was published in October 1992 as a document with four main parts: explanatory memorandum, directive (recitals and articles), financial statement, and impact assessment form.

The Second Proposal dealt only with the Directive and not with one of the other initiatives found in the initial package of the Commission. The decision in the field of information technology security already passed the Council in March 1992[58] because no co-operation process was necessary. The Directive on data protection in the field of telecommunication might be passed by the end of 1996.

---

52. Council Directive 95/46, art. 6, 7, 1995 O.J. (L 281) 31.

53. Working Party on Economic Questions (Data Protection)(on file with author).

54. Opinion on the Proposal from the Commission to the Council for a Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1991 O.J. (C 159) 38.

55. Opinion on the Proposal from the Commission to the Council for a Directive concerning the Protection of Individuals in Relation to the Processing of Personal Data, March 11, 1992, PE 160.503.

56. *See Dresner*, 20 PL&B 1992, at 14-15.

57. Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1992 O.J. (C 311) [hereinafter Amended or Second Proposal].

58. Decision in the Field of Security Information Systems, 1992 O.J. (L 123) 19.

On the basis of the Second Proposal, the Council discussed the Directive and decided on the Common Position on February 20, 1995. In the second part of the decision-making process, the Council passed the Common Position and an explanation to the Parliament.[59] The Parliament approved the Common Position on June 15, 1995, but proposed seven amendments. On July 24, 1995 the Commission accepted the amendments of the Parliament and passed the final Directive. The document had been signed by the President of the Council and approved by the Parliament on October 24, 1995. The final title is *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 Such Data.*

D. General Discussion

The proposals of the Directive caused a widespread discussion about data protection in Europe. None of regulations in the Member States met the requirements of the First Proposal. The Directive was discussed by the Parliament, the Member States' governments, Data Protection Commissioners, industry organizations and other groups concerned. They gave their opinions to the Commission in order to enable it to prepare the final Directive.

1. *Council Group on Data Protection and Government Statements*

A group of national government specialists on data protection and representatives of the Commission was founded to discuss in advance problems which could turn up later in the final decision of the Council. The group, "Working Party on Economic Questions (Data Protection)," discussed the national viewpoints in several meetings and members' working papers.[60] The working group prepared the conclusions and outcomes of the discussions in order to give them to the Commission.[61] These documents are not officially published and restricted; however, the Working Group played an important role in the process even though the Group does not have explicit powers under the EC-Treaty. The influence of the Group is based on the fact that the government specialists in the Working Party give advice to the representatives in the Council and the Council decides the Common Position and the final Directive.[62]

---

59. EC Treaty, art. 149 (2) (b).

60. Working Party on Economic Questions (Data Protection), *supra* note 53, at Working Documents.

61. Working Party on Economic Questions (Data Protection), *supra* note 53, at Outcome of Proceedings Documents.

62. Treaty of Rome, art. 189(b) (1957, as amended 1994).

2. *European Parliament*

The Parliament issued the First Proposal of the Directive for further discussion to the Committee on Legal Affairs and Citizens Rights. The Committee assigned one of his members, Geoffrey Hoon (U.K.), to prepare a report about the proposed Directive. The Hoon report was then discussed in the Committee and presented to the Parliament.[63] On the basis of the report, the Parliament discussed the Directive and recommended more than 100 changes in the proposed Directive.[64]

Three years later, the Parliament had made a decision about the Common Position. The aim of the involvement of the Parliament in the second reading of a directive is to give them the possibility to check whether their recommendations in the First Reading had been included. The Committee on Legal Affairs and Citizens' Rights discussed the Common Position in April and May 1995. The first reporter, Geoffrey Hoon, left the European Parliament and the Committee appointed Manuel Medina Ortega from Spain to check the Common Position. Based on his report, the Committee proposed that the Parliament pass the Common Position with only seven minor changes.

A comparison between the First Proposal and the Common Position shows that only few of the more than 100 amendments of the Parliament had been taken into account by the Commission. The main reason for the silence of the Parliament on that fact might have been caused by the absence of the former reporter, Geoffrey Hoon. On the other hand, the Parliament might have accepted that the Common Position was a very balanced and difficult compromise between the representatives of the Member States. Any major amendments by the Parliament would have created a substantial risk to the goal of getting the final Directive passed. The whole development is typical for decisions of the European Union and shows the substantial differences as compared to national democratic systems.

3. *Data Protection Commissioners*

Some countries of the European Union with data protection legislation appointed public data protection commissioners or supervisory authorities. Their responsibilities and powers differ between Member States. In 1989 the data protection commissioners demanded a Euro-

63. Report of the Committee on Legal Affairs and Citizens Rights on the Proposal from the Commission to the Council for a Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, DOC-DERR121809, PE 148.286/final, at 4 [hereinafter Report of Committee].

64. Opinion of the European Parliament of March 11, 1992 O.J. (C 94) 198.

pean data protection regulation.[65] One year later, the First Proposal was published and the commissioners complained that they had not been consulted for discussion.[66] They decided to take part in the further process of discussion.[67] The commissioners discussed the First and the Second Proposal in several informal meetings and gave comments.[68] However, the recommendations of the Data Protection Commissioners have no legal position in the decision-making process. In an April, 1995 meeting the Commissioners asked the Parliament to pass the Directive without major changes.[69]

4. *Other Statements*

The first reactions on the proposal came from industry organizations. These organizations were concerned about several provisions in the First Proposal.[70] The Commission asked those organizations to make comments on the Directive to the Commission.[71] The industry groups were concerned about the strong provisions for private businesses and some groups wanted to have their data processing excluded from the Directive or wanted to see special provisions and exemptions. The statements of the interested groups found their way to the Commission through committees[72] or directly to the Commission.[73]

---

65. Data Protection Comm'rs, Remarks at the 11th Conference of Data Protection Comm'rs (Berlin, Aug. 30, 1989) (on file with author).

66. Data Protection Comm'rs, Remarks at the 12th Conference of Data Protection Comm'rs (Paris, Sept. 19, 1990) (on file with author).

67. *Id.*

68. *See Dresner, supra* note 56, at 24.

69. EU-Data Protection Comm'rs, Remarks at the 13th Conference of Data Protection Comm'rs, (Lisbon, April 6-7, 1995) (on file with author).

70. *See Arbeitsgemeinschaft für wirtschaftliche Verwaltung*, AWV-I 12/1990, at 1; *Arbeitsgemeinschaft für wirtschaftliche Verwaltung*, CR 4/1991, at 256; *Deutsche Vereinigung für Datenschutz*, CR 5/1991, at 318; *Gesellschaft für Datenschutz und Datensicherheit*, Bedenken gegen den Vorschlag einer EG-Datenschutzrichtlinie, Mitteilungen der GDD 1/1992, at 2; *Gesellschaft für Datenschutz und Datensicherheit*, Stellungnahme zu EG-Datenschutzrichtlinie, 1990, at 1; *Hamburger Datenschutzkreis*, Stellungnahme zu den Artikeln 11 und 26 des Entwurfs einer EG-Richtlinie zum Datenschutz, 1992, at 1; *International Chamber of Commerce*, CLSR 6/1992, at 259; *Union of Industrial and Employers Confederation of Europe*, CR 2/1991, at 125; *Zentralausschuß der Werbewirtschaft*, Stellungnahme, 1990, at 1.

71. *See Dresner, supra* note 56, at 11.

72. *See* Amended Proposal, *supra* note 57, at 129.

73. *Id.*

IV. THE 1995 DIRECTIVE

A. Basic Ideas

1. *Rights and Freedoms*

On July 24, 1995, the European Commission finally decided on the European Directive for Data Protection.[74] The Commission initialized the Directive to secure an equivalent level of protection for personal data among the Member States.[75] The Commission claims two reasons for the initiative: first, the possibility that different levels of data protection laws could cause obstacles for border crossing data transfers,[76] and second, the protection of fundamental rights and freedoms within Europe.[77]

The Internal Market[78] and the co-operation of Member State public authorities raises the need for data transfers and especially, transfer of personal data within the Community.[79] Therefore, the Directive is needed to ensure the free flow of data by initiating a harmonized legal standard of data protection regulation in all Member States.[80]

The First Proposal provided a strong regulation with regard to constitutional aspects of privacy and Article 8 of the Human Rights Convention. However, the final Directive seeks to provide a framework, rather than minute provisions, in order to give Member States more independence.[81] During its development the Directive changed from precise provisions to a framework regulation. Nevertheless, the purpose of the Directive remains to regulate the duties as to information about the subject, requirement of consent, right to access, right to object, registration, and supervision. The final Directive simply gives a broader choice of measures to meet the requirements. In some cases Member States may pass their own regulations on the basis of their legal traditions.

The Directive protects the right of privacy within Europe in a new dimension. In the U.K. the Directive fills in a constitutional gap because (with some exceptions), the U.K. does not recognize a general right of privacy.[82] Greece and Italy have to introduce a data protection act for the first time. Countries outside the EU have to change their own stan-

---

74. *See generally* Council Directive 95/46/EC, 1995 O.J. (L281)31.

75. *Id.* at 8.

76. *Id.* at 7.

77. *Id.* at 20.

78. Treaty of Rome, art. 8(a) (1957, as amended 1994).

79. Council Directive, *supra* note 74, at 5.

80. *Id.* at 6.

81. Changes of the Proposal for a EC Protection Directive, Information Memo of the Spokesman's Service, October 23, 1992 [hereinafter Changes of the Proposal].

82. Adrian Sterling, Remarks at the IBC Data Protection Conference, London (Nov. 25, 1992)(on file with author).

dards, if they want to avoid obstacles in the exchange of personal data with countries of the European Union.[83]

The goal of the Directive is to protect "the rights and freedoms" of persons with regard to the processing of personal data,[84] in particular their rights of privacy. The regulation is based on Article 1 of the CoE Convention. The Directive refers[85] to Article 8 of the Human Rights Convention[86] which contains only the right of privacy. However, both the Directive and the CoE Convention also protect rights other than privacy. For example, the Directive deals with the question of lawfulness of an automated decision where such a decision might affect rights of freedom. Therefore, the Directive protects not only the right of privacy but also the right of freedom in general. Data processing can infringe upon the right of freedom in different ways. Consequently, pure protection of privacy would not solve all problems of processing personal data.

2. *Free Flow of Personal Data*

Article 1(2) shows one of the fundamental interests and ideas of the Directive: "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded effort under paragraph 1." The regulation prohibits Member States from restricting the free flow of data on the grounds of a less qualified level of protection in another country. The importance of the free flow of data aspect changed during the development of the Directive. Accordingly, the title of the Directive was changed in that respect between the First and the Second Proposal. The words "and on the free movement of data" were added to the original title.

The Directive intends to ensure an equal level of protection in national laws. However, it is questionable whether the Directive will reach this goal. The regulations must be accepted and used in public and the supervisory authorities must work properly. It is clear that data protection in the European Union will never reach the same standard because at least the interpretation of the balance of interests clauses depend on the value of data protection in the societies of each Member State. Furthermore, in practice, the national habits to meet the legal provisions will cause differences. The Directive tries to solve such problems by introducing a Working Party at the European Union.[87] However, it has not been given sufficient power. Only the European Court of Justice has

83. Council Directive, *supra* note 1, art. 25 (non-member countries have to provide a "adequate" level of protection).

84. *Id.* at art. 1(1).

85. *Id.* at 10.

86. SIMITIS, *supra* note 6.

87. Council Directive, *supra* note 1, art. 29.

the power to rule on a harmonised interpretation of the Directive. The rules on "direct effect"[88] of Directives might be used, however, that is not enough to replace every difference in implementation and interpretation of the Directive. Especially in the private sector, the instrument of direct effect does not work. There is only an obligation for judges to interpret the present law, as far as possible, in the light of a directive.[89] Finally, the process of obtaining a decision by the European Court of Justice is far too slow for the pressing need.

Sectional regulations in national laws could also cause different levels of protection, and therefore, create an obstacle in the sense of Article 1(2) of the Directive. Article 5 deals with the question of regulations in specific areas of national laws. Member States may "more precisely" determine the conditions in which the processing of personal data is lawful. There was no regulation like this in the First Proposal. However, when the First Proposal was published, Commissioner Martin Bangemann pointed out that the Directive provides, in some cases, for a minimum-standard.[90] In any case, it is not clear which scenarios are anticipated by Article 5.

The question of whether and to what extent the Directive provides an equivalent standard is quickly raised in Member States where the national law already provides sectoral regulations. If those regulations fall below the level of the Directive, they must be amended.[91] However, some specific regulations are stricter than the Directive. For example, German labour law defines some requirements for the lawful collection of employee data, and there are special rules for collective bargaining. Furthermore, in the public sector, specific regulations in Germany are stricter than the Directive.

3. *Public and Private Sector*

One of the main changes between the First and the Second Proposal was that the Second Proposal made no general distinction between the public and private sector. The OECD Guidelines, the CoE Convention, and most national laws[92] cover the public and private sector in the same provision. However, German law provides, with the exception of the first chapter, different regulations for the private and public sector, while Danish law has two different data protection acts concerning the private and public sector. In the U.S., the Privacy Act does not cover data pro-

88. Van Duyn v. Home Office 1974 E.C.R. 1348; Fancovich & Boniface v. Italy, 1992 I.R.L.R. 84; Marleasing v. La Commercial 1990 ECR 4135.

89. *Marleasing*, 1990 ECR at 4159.

90. *Bangemann*, *supra* note 46, at 11.

91. Council Directive, *supra* note 1, art. 8 (In the case of sensitive data the exemptions in the law have to meet the guidelines in Article 8).

92. Blume, *supra* note 13, at 401.

tection in the private sector. This shows the different approaches on the privacy issue— some countries do not distinguish between the protection against the state authorities or private businesses. In other countries, the legislature lets businesses stay as free from regulations as possible.

The human rights provisions[93] of the Directive draws an important distinction between the public and private sector provisions. Human rights deal basically with the relation between public authorities and citizens, but, protection of citizens against citizens is not directly covered by human rights. Therefore, the public and private sector have different backgrounds in the Directive. Moreover, the private sector is able to claim its own constitutional rights. Data protection regulations might effect businesses in their rights of freedom, especially the rights to carry out private enterprises and own property. Therefore, the legal precepts of data protection regulations for the private sector are not similar to those for the public sector.

The question, then, is whether the differences between the public and private sector have to lead to separate provisions in these fields. For example, in Germany, the constitutional impact of data protection leads to stronger provisions in the public than in the private sector. But the constitutional right of privacy is not only a defence against public authorities. It also makes governments responsible to protect the privacy interest of citizens against any threats. The Directive follows a similar approach based on the recommendation of the Economic and Social Committee[94] and points out that the individual has to be protected regardless of whether the threat is caused by public authorities or other citizens.[95]

Even without a general distinction between private and public sector, the Directive still accomplishes distinction.[96] For example, Article 3(2) excludes the application of the Directive for activities which fall outside the scope of EC law. Nevertheless, the private sector is totally covered. Therefore, the distinction between private and public sector is needed in order to define the scope of the Directive. This distinction is also needed for Article 7 of the Directive, which regulates the criteria for lawful data processing, because some of the provisions only make sense for the public sector. That holds true for Article 7(e), which regulates the data collection for public interest and in the exertion of public authority.

---

93. Council Directive, *supra* note 1, rec. 5.

94. Opinion on the Proposal from the Commission to the Council for a Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 199 O.J. (C 159) 38.

95. Changes of the Proposal for a EC Protection Directive, Information Memo of the Spokesman's Service, October 23, 1992.

96. *See* Ferdinand Kopp, *EG-Datenschutzrichtlinie*, DATENSCHUTZ-BERATER, Nov. 10, 1992, at 1.

The examples show that the distinction between private and public sector is still used in the Directive. It is impossible to regulate data protection without such a distinction, because the legitimate reasons for data processing of both sectors are different.[97] Therefore, the Directive cannot avoid the problem to draw the line between both sectors.

B. General Provisions

1. *Protection of Personal Data*

Article 2 of the Directive provides definitions for expressions used in the Directive. The function of the definitions is not only to repeat the general understanding of the words but to regulate their legal effect. The definitions differ from those which can be found in present data protection laws. The definitions of "personal data," "processing," "filing system," and "data subject's consent" can change the scope of the regulation rapidly.

Some of the key definitions of data protection regulations are of "personal data" and "filing system." A main change between the First and the Second Proposal can be found with regard these definitions. In the First Proposal, most of the provisions used the word "file." Then the Parliament suggested that the concept of a "file" should be dropped. The Second Proposal and the final Directive applies to "personal data" in most of the provisions. However, the definition of "filing system" is still used in relation to manual data: Article 3(1) restricts the scope of the Directive[98] to those forms of manual data which are part of or are intended to form part of a filing system.[99]

The intention of the Directive is to protect "personal" data. The definition of "personal" data is clear as long as the name of a person or an identification number is used. The First Proposal saw no reason to cover data without such a connection to the subject.[100] However, Article 2(b) of the First Proposal defines "depersonalization" in such a way that deletion of the person's name or identification number qualified as a depersonalization. Data therefore had to be changed so that the information could no longer be "associated" with a specific individual. Such an association is possible if information about the citizenship and employer are given. The definitions in Article 2(a) and 2(b) were not coordinated because of the distinction between data which is depersonalized before processing and that which is depersonalized after processing.

---

97. *See* Blume, supra note 13, at 401.

98. Council Directive, *supra* note 1, art. 29.

99. The important question of the extension of the scope to manual data is discussed *infra*.

100. First Proposal, *supra* note 3, art. 2 (a).

The Second Proposal deleted the definition of "depersonalization" and adopted the definition of "personal data." Personal data are "identifiable" if the person can be directly or indirectly identified. The definition is more expansive than in the First Proposal. Thus, the question of whether data is depersonalized is answered after determining whether it falls under the definition of personal data or not. The definition of depersonalization remained unchanged in the final Directive.

2. *Processing*

A precise definition of "processing" is likely to cause problems in data protection legislation because of future changes in the technology. In order to provide a preventive effect the Commission chose several phrases to describe processing. The meanings of these phrases overlap in order to avoid gaps in the regulation.

The Second Proposal did not only provide more overlapping phrases but differed in the total extent of the definition. "Collection," "organizing," and "consultation" of data were now included. The extension of the definition was based on Amendment 15 of the Parliament.

In comparison the CoE Convention excludes the collection of personal data from the basic principles of Chapter II. However, in the event of transborder flows of personal data, an extension is made. According to the Explanatory Report,[101] this was "considered indispensable in order to preclude data gathered in one country and processed in another from escaping the rules set out in this convention."[102]

The definition of "collection" is important for data collected in the European Union and then transported to another country. For example a U.S. company could make a survey by post. Under the First Proposal, the collection would not be included and the survey could be made without meeting the requirements of the Directive. However, the final provisions cover the collection of data transferred to third countries.[103]

3. *Controller and Processor*

The Directive builds up a distinction between the "controller" and "processor" of a data collection. The distinction was recommended in Parliament Amendment 18. The distinction is important in two situations: first, if the controller uses a third party to supply the data processing for him, and second, if the controller or processor is not located in one of the countries of the European Union.

---

101. Explanatory Report on the Convention of Europe, 1981 [hereinafter Explanatory Report].

102. NUGTER, *supra* note 12, at 28.

103. Council Directive, *supra* note 1, art. 25, 26.

4. *Manual Data*

The historical development of data protection initiatives shows that the specific risks of new technology provide reasons for these initiatives. Therefore, it seems clear that data protection provisions apply only to electronically stored data. Data need protection because they can be quickly copied, transmitted and merged. Manual data are less likely to be used in this manner simply because of the amount of time and effort needed. The Directive recognizes in Recital (4) that the progress made in information technology makes the processing and exchange of such data considerably easier.

However, even if the data protection discussion was caused by the development of new technology, the human rights idea of privacy applies to all kinds of personal data. Article 8(1) of the CoE Human Rights Convention[104] establishes a general right of privacy which can be infringed by personal data in any form. The Commission argues that manual files could be as dangerous as those in automatic files.[105] Therefore, the scope of the Directive should apply to all sorts of data but should also consider the difference in its nature.

The OECD Guidelines regulate only automatically processed data[106] and the CoE Convention applies in principle only to automated personal data files, but Member States are free to declare that they will include manual data.[107] The English Data Protection Act ("DPA") applies only to automatically stored data and the German Bundesdatenschutzgesetz applies only in some circumstances to manual data. However, the early Parliament Resolutions[108] and the final Directive cover manual data to some extent.

Data protection regulations should not obstruct the development of technology by supporting manual data with a general exemption. The OECD has argued that the regulation of only automatic data does not have the effect of obstructing the use of information technology.[109] However, no reason was given for that conclusion. In the U.K., the change from manual to electronic processing causes a new situation for the user because at present only electronically stored data are covered by the obligations of the English DPA. The user of a computer must register the use and comply with the data protection principles. The distinction between manual and electronic data might be a potential obstacle for the

104. Convention, *supra* note 17.

105. Changes of the Proposal, *supra* note 81.

106. *OECD Guidelines*, *supra* note 9, § 3(c).

107. NUGTER, *supra* note 12, at 26; SIMITIS, *supra* note 6, § 1 n.6 at 123.

108. *Resolution on Protection*, *supra* note 37, at 140.

109. SIMITIS, *supra* note 6, § 1 at 144.

use of new technology because if the electronic processing is unlawful, manual files may be used.

The Directive covers manual data but also provides some distinctions and modifications for them. First, the definition of "filing system"[110] in connection with Article 3(1) excludes main parts of the manual data from some provisions. "Personal data file" means "structured" sets of personal data, which are "accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." Moreover, the Directive states in Recital 27 that it covers only filing systems, "not unstructured files."

Article 18(5) deals with an exemption for personal data files. Member States are allowed to restrict the requirements of notification for non-automatic data files. The Commission gives no reasoning for the exemption in the explanatory part of the Second Proposal. The regulation is also not covered by an amendment of the Parliament. However, the possibility to exclude manual data from notification allows Member States to restrict bureaucracy.

In order to avoid problems for countries that have not yet covered structured manual data files in their data protection acts yet, Article 32(2) provides a derogation of the main regulations on manual data for twelve years from the date on which it is adopted.

5. *Exemptions from the Scope*

i. Private and Personal Activities

The First Proposal in Article 3(2) provides two main exemptions from the scope of the Directive. These exemptions excluded "non-profit-making bodies" and use for "purely private purposes" from the scope of the Directive. The Parliament Recommendation deals with these exemptions in two amendments.[111] In Amendment 22, the Parliament claims a change of the regulation to exclude purely private "use" and the Commission accepted this modification. The final version of the Directive excludes data held by a natural person in the course of a purely personal or household activity.

The development of electronic and manual diaries gives rise to the question whether or not they fall under the private activity exemption. The Commission seems to answer this question in the commentary part of the Second Proposal: "The second exemption concerns the use of data in the course of a purely private activity, such as an electronic diary."[112] However, such a general exclusion of electronic diaries is unlikely be-

110. Council Directive, *supra* note 1, art. 1 (2).

111. Parliament Recommendation, amends 22 and 23, Opinion of the European Parliament of March 11, 1992 O.J. (C 94) 198.

112. Amended Proposal, *supra* note 57.

cause of the technical possibilities to use those diaries and the reasoning behind Article 3(2). Modern electronic diaries are capable of storing more data than a desktop computer of ten years ago. They can include personal notes about employers or customers. Such use of an electronic diary is clearly business use in addition to private use. Therefore, a general exemption of electronic diaries is not ruled on by Article 3(2).

Even if Article 3(2) does not provide any general exemption for the use of electronic diaries, it is possible to argue for exemptions to a certain extent. While the Commission's proposal addresses an electronic diary, it possibly means a classic manual diary in electronic form. Such a diary is generally kept not only for private but also for personal business purposes. Therefore, the words "personal or household activities" might be stronger in their meaning than intended by the Commission, otherwise, the exemption would have no effect for electronic diaries.

ii. Press

Constitutional rules in the countries of the European Union protect the press and religious groups from obstructions by the public authorities. These protections have an important impact on data protection regulations. For example, the freedom of the press is protected in Article 5(1) of the German Constitution. The German Data Protection Act provides special exemptions for the press especially in view of the power of the supervisory authorities. Freedom of the press does not only relate to the possibility to publish without public control, but also to collect, store and use data. The Human Rights Convention[113] covers the protection of the press in Article 10.

The Directive provides an exemption for journalistic purposes or the purposes of artistic or literary expression in Article 9. One important question relating to the discussion about Article 9 is whether and to what extent the provision is an "obligation" for the Member States. The wording is "shall provide exemptions or derogations" from specific chapters of the Directive. The comparison with the provisions in the First Proposal ("may grant") shows that it is an obligation for the Member States.[114] However, the obligation is not drafted in detail. Therefore, the Member States have a wide range of discretion to comply with it. But since Recital (1) of the Directive refers to the Human Rights Convention,[115] the duty to provide exemptions for the press must be seen in the light of Article 10 of the Human Rights Convention.

113. Convention, *supra* note 17.

114. Amended Proposal, *supra* note 57, at 19.

115. Convention, *supra* note 17.

iii. Non-Profit Organizations

The First Proposal excluded non-profit companies from the Directive. Those companies cause fewer potential risks for the subject since they do not have personal economic interest in the processing of data. The exemption can help those organizations to work more effectively, however, there is no guarantee that non-profit organizations do not harm privacy rights. The marketing concepts of those organization are similar to those of normal businesses. Another problem could be that non-profit organizations might be used by for-profit businesses in order to provide collections of personal data.

In Amendment 22, the Parliament criticized the exemption. In the Second Proposal, the general exemption was deleted and a specific exemption was added in Article 8 of the Directive. The exemption in Article 8 takes into account that sensitive data are stored in the course of normal activity of organizations, unions or religious organizations.

C. GENERAL RULES ON THE LAWFULNESS OF DATA PROCESSING

1. *Principles on the Quality*

a. Fair and Lawful

In Article 6, the Directive states the principles related to data quality. These five principles convey basic ideas of data protection. The first principle requires that data processing should be done "fairly and lawfully." That has to be seen in context with the specific provisions in the Directive. The duties to inform the subject[116] relate to "fairly" and the stated grounds[117] for data processing to "lawfully." The other principles deal with the legitimate purpose, correctness, and deleting of data.

The function of the "principles" is difficult to define, because the Directive provides specific provisions. The Directive has implemented the idea of data protection principles from the CoE Convention. Article 5 of the CoE Convention covers the following principles:

> Personal data undergoing automatic processing shall be
>
> a. obtained and processed fairly and lawfully;
>
> b. stored for specific and legitimate purposes and not used in a way incompatible with those purposes;
>
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
>
> d. accurate and, where necessary, kept up to date; and
>
> e. preserved in a form which permits identification of the data subjects for no longer then is required for the purpose for which those data are stored.

116. Council Directive, *supra* note 1, art. 2(h) 10-12.

117. *Id.* art. 7.

There are some general differences between the Directive and the CoE Convention (e.g. extent of the scope on manual data). However, the principles cover the same ideas for data protection. Article 5 of the CoE Convention sets out some of the rules found in the eight Data Protection Principles in the U.K. Act.[118] The English Data Protection Act covers such matters as the requirement to obtain and process personal data fairly and lawfully; to ensure that data are adequate, relevant and not excessive; accurate and; where necessary, kept up to date. In contrast, the German Data Protection Act provides none of these principles. Instead the German Act provides specific provisions for lawfulness in order to reach its level of protection.

The extent of specific provisions in the Directive leaves little latitude for the use of the data protection principles. However, according to the view of the Commission, it might be necessary to refer back to Article 6 in order to interpret the subsequent articles in the chapter.[119]

The first principle asserts that the data processing must be fair and lawful. In the First Proposal, the principle also mentions data collection. This is important because the Directive does not explicitly pertain to data collection. However, in the Second Proposal, Article 2(b) of the Directive includes data collection in the definition of data processing. The question remains as to what purpose the first principle will have.

In the CoE Convention and the English Act, the main function of the equivalent principle is to cover the data collection. The Data Protection Registrar gives the first principle an important function with regard to fair access.[120] The Registrar takes the view that fair processing will require judging by reference to the purpose of the processing, the nature of the processing itself, and to its consequences for the individual affected by it.[121]

As an example of unfair processing, the Registrar mentions the use of unsolicited marketing material. In the Directive, this would be more a question of the legal ground of processing.

The German Act covers the collection of data only for the public sector. In the private sector Section 28(1), sentence 2 rules that data must be collected in "good faith." The interpretation of the regulation in the private sector is not yet clear. One commentator on the German Act real-

118. Data Protection Act, 1984, Schedule 1, Part I (U.K.).

119. *Commission of the European Communities*, Explanatory Memorandum, COM (92) 422 final at 2 (14) [hereinafter Explanatory Memorandum].

120. *Data Protection Registrar, in* Guidelines to the Data Protection Act 1984, Guideline 4, at 6 (1992).

121. *Data Protection Registrar, in* Guidelines to the Data Protection Act 1984, Guideline 4, at 11 (1992).

ises the function in preventing hidden collection.[122] Additionally, another commentator believes that the regulation provides in some cases for a duty to collect data from the subject and not from a third person.[123] However, direct collecting from the subject is not held to be a general duty. Such a general duty is only required in Section 13(2) of the German Act for the public sector.

The Commission provides examples for the function of the first principle.[124] Article 6(1)(a) should exclude the use of concealed devices or clandestine processing operations. However, in such cases, the question of the legal ground of collection already arises. Therefore, Article 7 of the Directive applies. And if consent is required, the user must provide information about the collection in order to obtain lawful consent.[125] But if the legal ground is not a consent but one of the other alternatives in Article 7, then the requirement of fair collecting could have some effect. Like in the German or the English Acts it could cover, in some cases, the principle of open and direct collecting. For example, the collecting of data from children of the subject could be treated as unfair.

b. Purpose

The limitation on lawful processing of personal data for a specific purpose is regulated by Article 6(1)(b) of the Directive. The Commission takes a strong view on the interpretation of the requirement. The purpose must be defined "before" data are collected and defined in "as precise a fashion as possible"[126] If the data are collected from the subject, Article 10 of the Directive requires that the subject must be informed about the purpose. The same holds true under Article 11 if the data are collected from third parties at the time they are stored. The description of the purpose should be detailed. The Commission gives, as an example, that the description "for commercial purposes" would be too broad.[127]

The English Act deals in the second principle with the purposes of processing: "Personal data shall be held only for one or more specified and lawful purposes."[128] Because the English Act is based on a registration system, the second principle refers to the purpose for which the processing is registered.[129] The registered purposes are not very specific because they describe the purpose for the whole processing, not for the

122. SCHAFFLAND & WILTFANG, BUNDESDATENSCHUTZGESETZ § 28 (1995) [hereinafter BUNDESDATENSCHUTZGESETZ].

123. *Id.*

124. Explanatory Memorandum, *supra* note 119, at 15.

125. Council Directive, supra note 1 art. 2 (b).

126. Explanatory Memorandum, *supra* note 119, at 15.

127. *Id.*

128. Data Protection Act, 1984, Schedule 1, Part I, § 2 (U.K.).

129. Data Protection Act, 1984, Schedule 1, Part II, § 2 (U.K.).

specific case. The German Act provides a strong limitation on the purpose of collection for the public sector.[130] However, in the private sector, the German Act is weaker. There is no general limitation on the purpose of collection. Only if data is transferred from a third person is the recipient bound by the purpose of transmission.[131]

The regulation in the Directive seems to be stronger than the present laws in Germany or the United Kingdom. However, it is very much a question of interpretation. It could be sufficient to specify the purpose more generally, but it could also be required to specify the purpose individually for every data collection. The second principle of the Directive demonstrates that there is a wide range of interpretations which may lead to different implementations in the Member States.

c. Correctness and Erasure

One of the basic concerns in relation to data protection is the correctness of data. The fourth principle of the Directive states that data must be "accurate and, where necessary, kept up to date."[132] The subsection states that "every reasonable step must be taken to ensure that data which are inaccurate or incomplete having regard to the purpose for which they were collected or for which they are further processed, are erased or rectified."

In comparison, the English Act deals in the fifth principle with the accuracy of data. The Registrar's view is that the principle obliges the user to take all reasonable steps to prevent the inaccuracy of the data.[133]

The German Act imposes a duty on the user to correct inaccurate data.[134] However, this duty itself does not imply the duty to provide measures in order to control the accuracy regularly. The commentators on the act are silent on this point. But, a general duty to take care in order to meet the provisions of the act can be found in Section 9. The user must take "the technical and organizational measures" necessary to ensure the implementation of the provisions of the Act. Based on this regulation the user must take measures to ensure the accuracy of data. Section 9 also provides a limitation for the efforts which have to be taken. Measures shall be required only if the effort involved is "reasonable in relation to the desired level of protection."

A difference between the Directive and the English and German Acts has been deleted in the Common Position of the Directive. Still, the

130. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 14(1).

131. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 28(4).

132. Council Directive, supra note 1, art. 6(1)(d).

133. *Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guideline 4, at 18 (1992).

134. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 20, 35.

Second Proposal of the Directive provided no limitation on reasonable effort or expense. The Directive required the taking "every" step to ensure accuracy. However, such a regulation would have been clearly disproportionate to the effect. In the final version, the Directive raises the duty to every "reasonable" step.

Closely connected with the purpose of the processing is the duty to erase data. The Directive points this out in the fourth principle. The English Act deals in the sixth principle with erasure. Data should not be kept longer than necessary for the purpose. The German Act[135] provides a similar duty for erasure in such cases. Since the duty for erasure is closely connected with the purpose, the effect of the provisions is dependent on the way the purpose is defined. The more specific the purpose is, the shorter the time limit for erasure. It could be argued that the English Act applies only to the erasure of complete files because "purposes" is defined for the whole file. However, the Registrar takes the view that the user has to look on the specific relation between the user and the subject.[136] Therefore, the Directive will not change the standard of the present English Act.

2. *Grounds for Data Processing*

The First Proposal of the Directive made a general distinction between the private and the public sector. Therefore, the lawfulness of data processing was regulated in different articles.[137] In the final Directive, there is one article for both sectors providing specific grounds for lawful data processing. Looking at the changes between the First and Second Proposal, the definition of processing has changed in a way that the collection of data is now included.

The regulation of the private sector in the First Proposal was criticized by industry as being too strict.[138] The Second Proposal also had to take into account several amendments of the Parliament.[139] It sought to abolish the distinction between the public and the private sector which was accepted by the Commission. The amendments are based on the old private sector provisions. The Parliament also proposed a different set of requirements for the communication of data. The distinction between communication and processing was deleted by the Commission because the Commission took the view that limitation of processing of personal

135. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 20(a), 35, 92.

136. *Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guideline 4, at 21-22 (1992).

137. First Proposal, *supra* note 3, arts. 6, 8.

138. *Arbeitsgemeinschaft für wirtschaftliche Verwaltung*, *supra* note 70, at 6; *Gesellschaft für Datenschutz und Datensicherheit*, *supra* note 70, at 8.

139. Parliament Recommendation amends. 28, 30, 31, 32, 33, and 34, Opinion of the European Parliament of March 11, 1992 O.J. (C 94) 198.

data on the defined purpose did not allow specific permission for communication.[140] However, there is an information requirement in Article 12 of the Directive which must be taken into account in cases of communication to third parties.

The Directive defines six alternative grounds for lawful processing of personal data:

1. consent
2. contract or entering in a contract
3. legal obligation
4. vital interests of the subject
5. public interest or in the exercise of official authority
6. legitimate interest

In the First Proposal, consent was held as the most important alternative of the alternative legal grounds.[141] In the Second Proposal, and in the final Directive, consent is one possible circumstance equivalent to the others.[142] Like the CoE Convention, the Directive balances the different rights and interests of individuals.[143]

The most important legal ground is placed in the sixth alternative. It deals with the fact that most of the data processing will not affect the interests of the subject in a substantive way. Therefore, strong requirements are not necessary in such cases. The Directive has chosen a system of liberal balance. The processing is only lawful if the interest of the subject does not "override" the interest of the user. The First Proposal provided a similar regulation.[144] However, the balance was limited on the situation that the interest of the subject did not "prevail." The Commission argues that the change of the regulation "has been drafted partly in response to Parliament's amendment no 32." But this amendment deals only with the communication of data and the Parliament had chosen a different balance. It required that "the interest of the data subject that warrant protection are not harmed."[145] There is no indication that the Parliament wanted to liberalize the balance. Moreover, the Parliament claimed that Article 8(1)(c) of the First Proposal should be deleted.[146] Therefore, the regulation in the Directive is contrary to the view of the Parliament.

As illustrated, the sixth alternative provides a liberal balance of interests. All the other alternatives are in practice only important for cases

140. Explanatory Memorandum, *supra* note 119, at 16.
141. First Proposal, *supra* note 3, rec. 11.
142. Council Directive, *supra* note 1, rec. 14.
143. *Council of Europe*, *supra* note 14, at 10.
144. First Proposal, *supra* note 3, art. 8(1)(c).
145. First Proposal, *supra* note 3, amend. (32), art. 8(2)(g).
146. First Proposal, *supra* note 3, amend. (32), art. 8(2)(g).

in which the legitimate interest of the subject overrides the interest of the user.

The first alternative, consent to the processing, must be seen together with the definition of consent in Article 2(h). The definition of the "data subject's consent" was not included in the First Proposal of the Directive. Instead Article 12 specifically provided for a regulation about the way consent should be given by the subject. The Second Proposal and the final Directive defines some requirements in the definition of the word "data subject's consent." In the Second Proposal, the consent required that the subject was given information about "the purpose of the processing, the data or categories of data concerned, the recipient of the personal data, and the name and address of the controller." However, the final Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." This version does not provide as strong requirements as the Second Proposal.

The second alternative deals with contractual relations. The processing is lawful as long as it is necessary for the performance of a contract. Data in question can only be those of the contractual partner and not of third parties. The difficulty of the regulation is based on the meaning of "necessary." The purpose of processing is usually widely defined but the contractual relation is quite specific. Therefore, the use of data for further marketing would be forbidden if there is no additional consent given by the subject.

Another question is whether it is "necessary" to use structured manual files or electronic processing. The use of electronic processing could be seen as disproportional compared with manual filing because electronic processing is more insecure with regard to data protection. A strong interpretation could lead to an obstacle for electronic data processing. The interpretation must take into account that the Directive recognises as its own purpose contribution to economic and social process, trade expansion and the well-being of individuals.[147] Therefore, the amount of data processed is limited by the word "necessary," but not the use of information technology.

The second alternative also provides a legal ground for processing in entering into a contract. Such an alternative is important in view of common trade practice. Otherwise, written consent would be required for quotations or information about products. However, because of the fourth principle of the Directive, data processed in the initial stages of a contract must be deleted soon thereafter.[148] One requirement of the reg-

147. Council Directive, *supra* note 1, rec. 2.

148. Council Directive, *supra* note 1, art. 6(d).

ulation is that the subject himself has requested the information. Otherwise, all marketing activities would be covered.

The First Proposal included processing necessary for a "quasi-contractual relationship of trust."[149] The regulation was copied from the German Act,[150] and the Parliament did not ask for a change of the provision. The Commission then argued that "many sources" considered the regulation as too vague.[151] From the U.K. point of view, the interpretation was difficult because there is no legal doctrine like a "quasi-contractual relationship" in U.K. law. Therefore, the Commission changed the regulation and limited its application.

The next alternative dealt with cases of vital interests of the data subject.[152] The regulation covers cases which are not included in the general balance of interest clause because there might be no legitimate interest of the user. For example, a person who wants to help a victim of a car accident has no interest because he acts only in the interests of the injured person. However, the interest to help in such a case could also easily be treated as a legitimate interest. Therefore, the regulation does not have any important effect.

Article 7(e) covers public sector processing and has a very wide application. The German Act restricts the lawfulness to cases in which the processing is necessary "to avert substantial detriment to the common weal or any other immediate threat to public safety." The First Proposal provided a similar regulation. The change in the Second Proposal was not backed by an amendment of the Parliament; moreover Amendment 30 shows that the Parliament wanted a clear mandatory requirement under the law. However, the Parliament did not object to this in the Second Reading of the Directive.

3. *Sensitive Data*

Article 8 of the Directive covers the processing of specific categories of data. Similar to the CoE Convention (Article 6), it requires special protection for classes of sensitive data, namely, those data revealing racial or ethnic origin, political affiliates, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. The CoE Convention rules that these data may not be processed automatically unless domestic law provides appropriate safeguards. The CoE Convention does not explain what is meant by "appropriate."[153] Thus, the Member States are free in the way they adopt the regula-

149. First Proposal, *supra* note 3, art. 8(1)(a).
150. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 28(1) No. 1.
151. Explanatory Memorandum, *supra* note 119, at 16.
152. Council Directive, *supra* note 1, art. 7(d).
153. *Criticised in* SIMITIS, *supra* note 6, § 1 ref. 120.

tion.[154] The Directive sets out five alternatives for lawful processing of sensitive data.

D. Rights of the Subject

1. *Information to the Subject*

i. Collection

Article 10 is the main regulation for information about the subject. Allready at the stage of collection, the user must give information about the identity of the controller and intended purposes. As far as necessary, the user also should give information about recipients, even where the replies to the questions are voluntary, and the subject enjoys access and the right to rectify. The question whether such information is necessary has to be judged in view of the specific circumstances in which the data are collected, to guarantee fair processing with regard to the data subject.

The Parliament did not propose significant changes to the First Proposal with regard to the information of the subject. Amendments 44 and 45 deal with the changes of the definition of data. Amendment 43 attempted to include "groups of individuals," but these data are already included since the definition of personal data includes identifiable data.[155] The Commission introduced one important change on its own: Article 13 in the First Proposal gave "the right to be informed." This could have been interpreted that information had to be given only on request. The Commission wanted to "clarify" that the information must be given to the subject without the need for request.[156] The change might not only be a clarification but there were good reasons to extend the duty of information, because the Commission introduced some exemptions for registration.[157] If the subject has less possibility to get information about data processing from the Registrar, then the duty to provide information is more important.

The Second Proposal of the Directive was stronger on the duty of providing information to the subject than the final Directive. All information had to be given regardless of whether it was necessary. This would have caused too much bureaucracy for simple cases of collection. Therefore, the Council changed the provision in the Common Position and the Parliament approved this change for the final Directive.

One of the basic data protection problems is the possibility to transfer data easily. Therefore, data protection provisions deal with the dis-

154. Simitis, *supra* note 6, § 1 at 120.
155. Council Directive, *supra* note 1, art. 2(a).
156. Explanatory Memorandum, *supra* note 119, at 20.
157. Council Directive, *supra* note 1, art. 19.

closure of personal data. The disclosure of personal data to a third party is limited on the legal grounds of processing. As an additional safeguard the user may be obligated to give information to the subject about the disclosure. The OECD Guidelines, the CoE Convention, the UN Guidelines, and the English Act do not provide specific regulations for such disclosure.

The proposed Directive provided a specific article regarding disclosure to third parties.[158] The title of the provisions changed in comparison to Article 9 of the First Proposal and Article 11 of the Second Proposal. Article 9 provided a general obligation to inform the subject. However, the provision dealt only with information to the subject provided at the time of first communication or opportunity for on-line consultation. Therefore, the obligation did not change in substance.

The Commission followed Parliament's Amendment 35 and changed details of the regulation in the Second Proposal. The obligation to inform was reduced to cases in which the purpose of the data processing is a contract, the law, or public and general interest. The obligation covers not only the private but also the public sector. The First Proposal mentioned on-line consultation but the regulation was deleted because the Commission took the view that on-line consultations were covered by the word "disclosure."[159] In the Common Position and the final Directive, the whole regulation changed. The final Directive provides a duty for the person who collects data from someone other than the data subject.

The Directive defines the information which must be given to the subject. The controller must provide the information at the time of undertaking the recording. However, if a disclosure to a third party is envisioned, the controller must give the information no later than the time when the data are first disclosed. The information must be given only if the subject does not have it already. Therefore, it is useful to provide such information at the time of collection.

If the data are not collected from the subject, Article 11 provides some exemptions from the duty of disclosure. No particular information need be given if the data involved processing for statistical purposes, historical or scientific research, or if the provision of such information proves impossible or would involve a disproportional effort. Another exemption is granted if the recording or disclosure is expressly required by law.

ii. Right of Access

The duty to inform and the right of access are two different methods to provide the subject knowledge about his processed personal data.

158. *Id.* art. 11.

159. Explanatory Memorandum, *supra* note 119, at 21.

However, the right of access is not helpful where the subject is unaware that his personal data are stored by someone. The right of access is an additional right in order to protect the subject's rights. The international agreements all regulate the right of access.[160] The German[161] and English Acts[162] also contain state provisions regarding access for the subject, but there are some differences in the details.

The first question to answer is which information the subject must give the user in order to assist in finding the personal data stored. The CoE Convention and the OECD Guidelines give no answer to the problem. The German Act provides a requirement for detailed information for the search in cases of access to manual data.[163] The UN guidelines give the right of access only to persons who give their "identities." That might require the person to give name, address and the day of birth. The English Act[164] provides a duty for the subject to give information for the location of the information. However, in the final Directive no exception is made. The duty of access is strict and will be quite difficult especially with regard to manual data files. Using search programs it would be easy to find electronically stored personal data. However, modern network systems have changed the structure of data files. Data storage may be decentralized and others centralized. Therefore, it would be quite complicated in practice to find personal data in a large size company if the subject provides nothing more than his name on the request.

Article 12 of the Directive creates the right to obtain information regarding the existence of the storage of personal data and the data itself. Like the international regulations, the Directive directs the data to be communicated to the subject in an "intelligible" form. There is no expressed obligation to present the data in a intelligible form in German or U.K. law. The British Registrar takes the view that the user should give an explanation if the data are not intelligible.[165] A German court[166] interpreted the right of access to mean that the subject has the duty to provide the data in a practical form. Therefore, the Directive will not change the present situations in Germany and the U.K.

In the First Proposal, the function of the regulation[167] was only to give a right of access to the information stored. Then the Parliament

160. *OECD Guidelines*, *supra* note 9, no. 13; *Guidelines*, *supra* note 29, § 4; Convention, *supra* note 17, art. 8.

161. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 6, 19, 34.

162. Data Protection Act, 1984, § 21 (U.K.).

163. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 19 (concerning the public sector).

164. Data Protection Act, 1984, § 21(4) (U.K.).

165. *Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guidance Note 5, at 7 (1992) [hereinafter Guidance Note].

166. Bundesarbeitsgericht (BAG), Der Betrieb (DB) 1988, at 133.

167. First Proposal, *supra* note 3, art. 14(4).

asked in Amendment 48 for the extension on the "general origin" and the "exact use." The amendment has been partly accepted by the Commission. Article 13 of the Second Proposal covered the information about an "indication" of the source and a "general information on their use." The German Act also provides for the right to obtain information about the sources after the Act was amended in 1990.[168] The reason for the German regulation is that the subject should be enabled to find out whether a transmission of data was lawful.[169] The German Act also provides the right to obtain information about the recipient of data transmissions. The information must include the name and address of the source or the recipient. Neither the international regulations nor the English Act give a right to obtain information about the source of the data.

The catalogue of information was changed again in the Common Position of the Directive. Now the controller must provide "confirmation as to whether or not data relating to him are being processed and information at least as to the purpose of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed."

One problem relating to the right of access is the cost of a search. In the U.K., the costs for information from one registered application is regulated to a maximum of £10.[170] The German Act provides for free access to personal data.[171] However, there are special provisions for those companies who deal with information for the purpose of supply to third parties. These include companies providing credit information. In such cases, the fees may not be higher than the effective cost of the search. The duty to pay the cost reflects the possibility that the subject will use the information for personal purposes. The reason for the regulation is that data subjects tend to use their right of access in order to get the information for personal use (e.g., to prove their financial reliability to the owner of a house which they want to rent).

The Directive states no precise limit for the duty to pay the costs of a search. Article 12(a) regulates that the costs should not be "excessive." In practice there is a relation between the duty to provide information which can help to find processed data and the duty to pay the actual costs of the search. The more difficult to find the data, the more the subject must pay for the search. Therefore, the subject has an interest in providing information in order to help the user to find the data.

There are two different ways to look at the words "excessive" costs. One way is the view of the subject. The costs are not excessive if they are

168. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 19, 34.

169. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 34, 39.

170. Guidance Note, *supra* note 165, at 4.

171. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 34, 50.

proportionate to the value of the access. The other is the view of the user looking at his own costs. However, in some cases such costs might be quite high, especially if the subject gives no detailed information about the data he is looking for. The wording of the Directive is similar to Article 9(b) of the CoE Convention. The official interpretation of the Convention regulation is that the user has only the right to charge a fee; but not the actual cost of the operation.[172]

Additionally, the time in which an answer must be given to the subject is important for the effectiveness of the access right. The U.K. time limit is forty days.[173] There is no equivalent regulation in German law. However, the regulation must be interpreted in a way that the information must be given in a limited time. Otherwise, the whole regulation would not work in the proposed way. The Directive now states that information must be given "without delay." In the Second Proposal, the text was "without excessive delay." The Council changed the wording in Article 12(a) of the Common Position, but it is questionable whether this change makes any difference.

The right of access must be granted in "reasonable intervals." There is no equivalent regulation in the German Act. The English Act provides that excessive "frequency" of requests will relieve users of the duty to respond without delay.[174] This provision in the Directive is taken from Article 8(b) of the CoE Convention. The explanatory report of the Convention discusses "fixed intervals" of information.[175] However, the reasoning of the regulation is to provide a limitation for the amount of requests rather than a fixed interval service. Member States are left to specify what are "reasonable intervals" in the sense of the Directive means.[176]

iii. Exemptions

The right of subjects to be informed is not absolute. However, there are different provisions for different rights. Article 13 refers to all information rights in Articles 10, 11, and 12.

Seven alternative situations for an exemption to the right of information and access are laid down in Article 13(1) of the Directive. The first three exemptions concern the national security, defence, criminal proceedings and public security. Similar provisions are found in the German[177] and English Acts.[178] These exemptions are mainly for the public

172. Explanatory Report, *supra* note 101, at 19.
173. Guidance Note, *supra* note 165, at 4.
174. Data Protection Act, 1984, § 21(8) (U.K.).
175. Explanatory Report, *supra* note 101, at 19.
176. Explanatory Memorandum, *supra* note 119, at 22.
177. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 19(4).
178. Data Protection Act, 1984, §§ 26-29 (U.K.).

sector and protect vital interests of the government.

The most vague exemption can be found under subsection (2)(g) of the Directive. In the Second Proposal the provision stated that information and access need not be given if there is an "equivalent" conflicting right of another person or the right and freedoms of others. This was changed by the Council in the Common Position. In the final Directive, the exemption is made when it is a necessary measure to safeguard "the protection of the data subject or of the rights and freedoms of others."

The controller of the data is included by the word "others." His rights might already be affected if high costs are connected to the information procedure. Therefore, the exemption could be important in relation to access to manual data, because in some cases a search for such data might be difficult and quite costly. In such a case, the equivalent interest could be the cost of the search.

2. *Right to Object*

The data subject's right to object is part of the right to control which data are stored about him. In order to control processing, he can refuse to give his consent to processing. But since there are some alternative legal grounds for the processing, the data subject might only be able to stop the processing later.

All data protection regulations provide sections about the right to object, but, they differ in their requirements. The CoE Convention gives the right to obtain if the data have been processed contrary to law.[179] The UN Guidelines grant the right to object if the processing is unlawful, or not necessary.[180] The OECD regulation is unclear, because the right to object is granted if the "challenge is successful."[181] That would only be the case if the processing is unlawful.[182]

Article 15 of the Second Proposal provided the possibility for the subject to object to processing on "legitimate" grounds. This has been changed by the Council. The final Directive obligates the Member States in Article 14 to grant the subject the right to object only in certain cases. In cases of processing for marketing purposes, the right to object has to be granted. But, if the legal ground for processing is based on public or personal interest,[183] the right to object exists only on "compelling legitimate grounds."[184] Article 14 does not obligate the Member States to

179. Commission Recommendation, *supra* note 35, art. 9(c).

180. *Guidelines*, *supra* note 29, § 4.

181. *OECD Guidelines*, *supra* note 9, § 13(d).

182. Charlton, ENCYCLOPAEDIA OF DATA PROTECTION, *Explanatory Memorandum* 7-237 (1995).

183. Commission Recommendation, *supra* note 35, art. 7(e), (f).

184. Explanatory Memorandum, *supra* note 119, at 25 (the commission seems to understand "legitimate" reasons also in the way that the processing is unlawful).

grant the right for objection in other cases, although they are free to do so.

E. Automated Individual Decisions

Article 15 of the Directive deals with automated individual decisions. The provision is not based on any international regulation. Only French law has a comparable regulation. The Commission tries to prevent the possibility that an automated decision could be made without the opportunity for the subject to control or even recognize the decision. It deals with the ethical impact of the possibility that computer decisions might replace human decisions.

The idea of Article 15(1) is that nobody should be subject to a "solely" automated decision. In the Second Proposal, the requirement had been that the decision adversely affects the subject. However, the Council considered the problem of defining what "adversely" means. An appropriate test would be to ask whether there was one possible decision better than the one taken. However, such an interpretation would cover nearly every decision.[185] As a result, the final Directive clarifies the meaning and requires that the decision "produces legal effects concerning him or significantly affects him." However, the interpretation problem still remains. One possible test would be to compare the situation before and after the decision in order to find out whether the position of the subject changed. In such a case, only a few decisions would be covered, but, not a negative decision about an overdraft at the bank. However, it would cover the decision to cut an overdraft. The Directive gives no answer where to draw the line.

The next problem is what the Directive defines as a "solely" automated decision. If a company wants to make an automated decision which is not *solely* automated it must provide that a human checks the outcome. The question is whether such a person should be entitled to make a different decision by himself or whether he would only have a control function. In each case it is quite difficult for the subject to prove if somebody has taken part in the decision or not. Therefore, the question is whether there is any chance for the provision to work effectively.

A more effective regulation with regard to automated decisions is Article 12(a), alternative 3 of the Directive which obligates the user to give knowledge of the logic involved in any automated decision. The provision is based on Parliament Amendment 46. The duty to give detailed information about the decision could raise problems if such reasoning includes company secrets or could create possibilities for fraud. How-

185. Marc Schauss & Jan Berkvens, *EC Commission Proposals on Data Protection: Continuing Threat to Financial Transactions*, Computer L. & Prac., 4, 98, 101 (1992) (arguing that automatic credit scoring would be prohibited).

ever, in such cases the exemptions of Article 13 apply and Recital 41 points out that trade secrets should not be affected.

F. Data Security

Data protection regulations cover the lawfulness of processing, but they must be assisted by technical measures to protect data against unlawful processing. The Directive provides a regulation for the security of processing in Article 17. They are not very specific and open for changes of the technology.

One important change between the First and the Second Proposal was that the new regulation does not take the costs of security measures into account.[186] The change has been criticized by industry representatives.[187] The final Directive takes the costs of security measures into account. The controller must choose a level of security having regard to the state of art and the cost of their implementation. Further, the "state of art" must be defined on a European Union level. Otherwise, it would cause different levels of protection in the Member States. A European Union-wide definition of the "state of art" might be given by security guidelines prepared by the Commission based on the decision on information technology security.[188]

G. Remedies and Liability

1. *Remedies*

Chapter III of the Directive deals with judicial remedies, liability and penalties. Such provisions can also be found in Article 10 of the CoE Convention, which requires Member States to establish appropriate sanctions and remedies for breach of domestic data protection legislation. The OECD Guideline[189] recommend that states make provisions for sanctions and remedies not only to ensure the protection of personal data — like the CoE Convention and the 1979 EC Resolution[190]— but also to deter actions which may interfere with their free circulation. The German Act covers penalties[191] for all unlawful operations under the Act. The U.K. law creates several detailed criminal offenses.[192]

The Directive identifies that remedies are important for the enforcement of data protection regulations. Article 22 makes clear that Member

186. Council Directive, *supra* note 1, art. 17(2).
187. *Confederation of British Industry*, CLSR 2/1993, at 74, 76.
188. Amended Proposal, *supra* note 57, at 123.
189. Bundesdatenschutzgesetz, *supra* note 122, § 19(b).
190. *Resolution on Protection*, *supra* note 37, at 140.
191. Bundesdatenschutzgesetz, *supra* note 122, §§ 43, 44.
192. *Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guideline 7, at 22-23 (1992).

States shall provide the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question.

2. *Liability*

Unlawful processing might cause damage to the subject. Article 23 deals with the question of liability. The 1979 E.C. Resolution[193] states that data users shall be liable "for material and non-material damages caused by the misuse of data whether or not there was negligence on his part." The English Act provides two compensation provisions,[194] one in the case of inaccuracy of data and one in the case of loss or unauthorized disclosure. The German Act distinguishes between the public and the private sector.[195] There are three main questions arising with regard to liability clauses: first, whether the liability is a strict liability or whether there is a special exemption; second, what sort of damage is covered; and third, if there is any limitation on the amount of compensation. The liability clauses in the Directive and the English and German Acts provides strict liabilities. However, there is a possibility for the user to prevent the liability if he proves that he has taken reasonable care. The German Act does not provide this exemption for the public but allows for the private sector. Under the Directive it is left to the Member States to decide whether they want to grant the possibility for such an exemption if a user can prove that he is not responsible for the event giving rise to the damage.

H. THIRD COUNTRIES

All international initiatives on data protection are designed to allow reasonable solutions for transnational data flow. The Directive solves the problem within the European Union by introducing a equivalent level of protection. There is no regulation like this in the CoE Convention or the OECD Guidelines. The U.N. Guidelines work with a general principle of "equivalence."[196] The German Act provides a specific regulation only for the public sector.[197] In the U.K., the Registrar has the power to refuse registration or to issue a de-registration notice if he is satisfied that the transfer or disclosure contravenes the principles of the English Act.[198]

Based on Article 1(2), no restrictions between the Member States are

193. *Resolution on Protection*, *supra* note 37, at 140.
194. Data Protection Act, 1984, §§ 22, 23 (U.K.).
195. BUNDESDATENSCHUTZGESETZ, SUPRA note 122, §§ 7, 8.
196. *Guidelines*, *supra* note 29, § 9.
197. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 17.
198. NUGTER, supra note 12, at 206.

allowed.[199] The Directive covers third country transmissions of personal data in Chapter IV. The First Proposal was criticized regarding the third country provisions by industry groups because of their inflexibility.[200] The Commission changed the regulation in the Second Proposal by introducing some exemptions. Data transfer to countries without an adequate level of protection is possible under several alternative situations. The exemptions were introduced by the Commission also in the interest of the consumer.[201] They remained, with some changes, in Article 26 of the final Directive.

Data transfer to countries without an adequate level of protection is allowed under Article 26 if:

> (a) the data subject has given his consent unambiguously to the proposed transfer, or
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request, or
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party, or
>
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
>
> (e) the transfer is necessary in order to protect the vital interests of the data subject, or
>
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Regardless of these exemptions, the requirement of an adequate level of protection will be important for a number of cases. Through that requirement the Directive has an impact well beyond the boundaries of the Community.[202] An adequate level will not mean the same level as within the Member State because the Member State level is "equivalent"[203] in the language of the Directive.

Subsection (2) of Article 26 defines the requirement of an "adequate" level. The definition was introduced in the Second Proposal in order to

---

199. *Council Directive*, *supra* note 1, art. 1(2).

200. *Gesellschaft für Datenschutz und Datensicherheit*, *supra* note 70, at 16; *see also Arbeitsgemeinschaft für wirtschaftliche Verwaltung*, *supra* note 70, at 2.

201. Changes of the Proposal, *supra* note 81.

202. Colin Tapper, *New European Directions in Data Protection*, 3 J. INFO. & SCI. 9 (1992).

203. Council Directive, *supra* note 1, at 2.

"clarify" the meaning of the third country regulation.[204] However, the definition of subsection (2) seems to be more than a clarification. There are two different ways to look at the level of protection. One is to look at it in a general way and to take into account the data protection measures in a country as a whole. The other way is to look at the specific processing and to see whether the measures taken are adequate. The First Proposal could be interpreted in the first way, but, subsection (2) of the Second Proposal makes clear that the regulation has to be interpreted in the second way. Therefore, the Commission will prepare a negative list of transfers for negotiations about regulations to secure adequate protection.[205] Some countries might not be able to meet the requirement for all transfers.[206]

I. CODES OF CONDUCT

Chapter V of the Directive provides the possibility for trade associations to produce additional provisions for specific sectors.[207] The OECD Guidelines[208] promote the idea of self regulations similar to the codes of conduct in Holland, Ireland, and the U.K.[209]

The main question about codes of conduct relates to their legal effect. The self regulation in the meaning of the OECD Guidelines[210] could be compensated by legislation.[211] In Holland and the U.K., codes of conduct have only an illustrative function.[212] The same holds true for the Directive. The codes represent guidance, acceptance is voluntary, and recommendations are not binding. Therefore, such codes of conduct are less important.

J. SUPERVISORY AUTHORITIES AND WORKING PARTY

1. *Member State-Level*

i. Registration and Derogations

The Directive uses a registration[213] system in order to reach a high

204. Changes of the Proposal, *supra* note 81.

205. *See* Council Directive, *supra* note 1, art. 25, § (5).

206. *See* Reidenberg, *Data Protection Measures in the United States*, 80 IOWA L. REV. 497 (1995).

207. Council Directive, *supra* note 1, arts. 28, 29.

208. *OECD Guidelines*, *supra* note 9, § 19(b).

209. *See Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guidance Notes 1,6 (1992).

210. *OECD Guidelines*, *supra* note 9, § 19(b).

211. SIMITIS, *supra* note 6, § 1, at 147.

212. *Data Protection Registrar*, *in* Guidelines to the Data Protection Act 1984, Guidance Note 6 (1992).

213. Council Directive, *supra* note 1.

level of data protection. The 1979 Resolution[214] already required prior registration or authorisation for the processing of personal data. However, none of the international agreements requires registrations as a data protection measure. The U.K. and the French laws work with a registration system. In Germany, registration is required for the public sector,[215] and in some cases in the private sector.[216] However, the main system in the private sector is based on data protection on the company level instead of registration.[217] The strong approach of the First Proposal towards registration was criticized in Germany.[218]

The registration has to be carried out before running the processing and has to include several specifications.[219] One change between the First and Second Proposal was that registration in the First Proposal was related to "files" while the Second Proposal describes "processing." The Parliament asked in Amendment 37 only for a change of the word "files" to "data." However, the Commission felt that in the "spirit" of the Parliament's opinion, the provision should be extended to all notified "processing." In the light of rapid technology developments, the registration of "files," as in the English Act, is not effective because the identity of files is changed during processes. Data base software uses several "files" to manipulate and several programs which are able to display data in different relationships to each other.

The First Proposal reduced the duty of registration in the private sector to those files which are intended to be communicated.[220] The Second Proposal skipped the requirement. The change remained in the final Directive. Therefore, all processing has to be registered regardless of whether it is intended to be communicated or not.

Article 21 gives the right to any person to inspect the register. The right to inspect covers all information in the register except for the information about security measures.[221] A second exemption is made under the requirements of Article 13.[222]

The system of registration in the First Proposal was criticized for being too strict and complicated.[223] Following the idea of Amendment 39, the Commission introduced Article 18(2-5) as a regulation for simplification and exemption from the obligation to register. However, the

214. *Resolution on Protection*, *supra* note 37, at 140.
215. BUNDESDATENSCHUTZGESETZ, *supra* note 122, §§ 26(5), 18(2).
216. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 32.
217. *Eickeler*, HANDELSBLATT, Nov. 12, 1992, at 4.
218. *Id.*
219. Council Directive, *supra* note 1 arts. 18(1), (2).
220. First Proposal, *supra* note 3, art. 11.
221. Explanatory Memorandum, *supra* note 119, at 33.
222. *Id.*
223. *Gesellschaft für Datenschutz und Datensicherheit*, *supra* note 70, at 10.

Commission did not follow the Parliament Amendment in detail. Member States shall provide exemptions for certain categories of processing. These processing categories must be specifically detailed according to subsection (2). The Commission's opinion is that 80% of all processing could be covered by such exemptions.[224] However, that would require a large amount of specified exemptions because it is not possible to describe large groups of processing in one exemption. The specification of the exemption must be detailed.

If registration is derogated then the subject still has the right to ask for information about data processing. Article 21(3) grants any person the right to obtain information about the existence of processing operations and detailed information about them. The only difference from an inspection of the public register is that the person has to question the controller directly. One of the industry recommendations on the Second Proposal asks for a change of the provision because there is no limitation that the person is a subject of the processing.[225] Therefore, the regulation might be used by competitors in order to get information about the data processing of a company. However, the aim of the access right is to provide information to the subject. In the Second Proposal it was proposed that only the subject has the right to ask for information about data processing which is related to him. However, the Council changed that in the Common Position. The Final Directive states that Article 10 is to give not only a present subject, but everybody the right of access.

ii. Rights of Control

The Directive obligates the Member States in Article 28 to build up a supervisory body for data protection. Under subsection 3, the authority must either obtain investigative powers and the right to engage in legal processing or bring cases to the attention of the judicial authorities. Additional power for intervention might be given to the authorities. The Directive provides several intervention options including the power of "delivering opinions before processing operations are carried out, . . . ordering the blocking, erasure or destruction of data, . . . imposing a temporary or definitive ban on processing, . . . warning or admonishing the controller, or . . . referring the matter to national parliaments or other political institutions." Based on the varying choices, it is likely that the Member States will grant totally different intervention powers to their data protection authorities.

The UN Guideline was the first international regulation calling for an independent control organization.[226] Member States with data pro-

224. Changes of the Proposal, *supra* note 81.

225. *Gesellschaft für Datenschutz und Datensicherheit*, *supra* note 70, at 4.

226. *Guidelines*, *supra* note 29, § 8.

tection laws already had such institutions, however, the functions and rights of those institutions are different. The English supervisory bodies are the Secretary of State and the Registrar. The Registrar is independent and might refuse entry to the register or issue a Registrar notice.[227] To conduct inspection visits and seize evidential material,[228] the Registrar requires a warrant issued by a judge to enter and search. The decisions of the Registrar can be verified by the Data Protection Tribunal. The German system of supervisory authorities distinguishes between the public and the private sector. The Federal Data Protection Commissioner has to control the federal public authorities. He is also responsible for the annual data protection report which covers the public and private sector. The Länder Data Protection Commissioners are responsible for processing in the Länder public authorities which have their own data protection acts. The whole private sector is controlled by public authorities of the Länder. They are not independent and control the public sector mostly on request of a subject. Their legal instrument is the German Bundesdatenschutzgesetz and specific laws.

The First and Second Proposal gave an independent supervisory authority substantial powers for investigations and interventions. The regulation was criticized by German supervisory authorities because an "independent" commissioner should not have investigation or intervention power.[229] Under the German constitution, public authorities must be under control of the Parliament or the government as far as they carry out supervisory functions in relation to the private sector. Under the proposed regulation in the Directive, they would have been only under control of the courts. Suddenly, the provision was changed in the Common Position.[230] In the final Directive the German system is allowed to remain.

The supervisory authority also has the duty to hear complaints by subjects and to answer. According to subsection 5, the Federal Data Protection Commissioner has to provide a report on the Commission's activities at regular intervals.

2. *Company-Level*

In Article 18 subsection 2, the Directive provides the possibility to grant exemptions from the duty of registration if a internal data protection commissioner is appointed. The regulation is based on the idea of

227. Data Protection Act, 1984, § 7 (U.K.); *see* Charlton, ENCYCLOPAEDIA OF DATA PROTECTION 1-041.

228. Data Protection Act, 1984, sch. 4, § 2 (U.K.).

229. *Oberste Aufsichtsbehörden der deutschen Länder*, Gemeinsame Stellungnahme zum geänderten Vorschlag der Kommission (1992), at 15.

230. Council Directive, *supra* note 1, art. 28.

the German Act. In Germany, data protection commissioners in the private companies are appointed to organize and control data protection. If a company in Germany has more than five people working on computers then the company has to appoint somebody who is in charge of data protection.[231] In large companies full-time commissioners are employed. In smaller businesses someone has the function of a data protection commissioner in addition to his normal job. Some businesses use lawyers as external data protection commissioners.

The German system is not a system of self regulation but a system of self control. The private Data Protection Commissioner is in charge of the preparation of a company register.[232] Companies have the duty to control data processing and to educate the staff in issues of data protection.[233] If someone has complaints about data protection, he can go directly to the commissioner. The commissioner himself has direct access to the management.[234]

If there are data protection complaints about a company, the data protection authorities have the power to control the company. The private commissioner then has the duty to prepare the material for the company and must give information about the data processing. The system is less bureaucratic than a national registrar and it has at least the same effect. There was no regulation in the First Proposal to support such a system of private Data Protection Commissioners. A provision about data protection commissioners on the company level was proposed in Germany.[235] Then, the exemption was introduced in the Second Proposal.

3. *European Union Level*

Under the Directive, there is no supervisory body for the whole of Europe. However, the Commission can use the provisions of the Directive for their own administration. Thus, the Commission proposed a declaration about the use of the Directive for the institutions of the European Community. A draft version of such a declaration was included in the package together with the First Proposal.[236] Under the provisions of the Directive, the Commission must build a supervisory body to control data protection at institutions of the European Commu-

231. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 36(1).

232. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 37(2).

233. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 37(1).

234. BUNDESDATENSCHUTZGESETZ, *supra* note 122, § 6(3).

235. *Geis*, CR 1/1993, 31, 34; *Schneider*, CR 1/1993, 35, 38.

236. *Commission of the European Communities,* Commission Declaration on the Application to the Institutions and other Bodies of the European Communities of the Principle Contained in the Council, COM (90) 314.

nity. The purpose of this body is only to look at issues of data transfer to third countries.

4. *European Union Working Group on Data Protection*

Under the chapter about supervisory authorities, two articles about a European Working Party on data protection are found.[237] However, the working party has only advisory status and will be composed by representatives of the supervisory authorities. The task of the Working Party is described in Article 30 of the Directive. The function is mainly to discuss the European problems of data protection and to give advice to the commission.

V. CONCLUSION

The Directive is one of several attempts for an international harmonization of data protection laws. Some of the provisions in the Directive were taken from the CoE Convention and some ideas arose out of the OECD and UN Guidelines. However, there are two main differences between the Directive and other international regulations: first, the legal effect; and second, the extent of the detailed provisions and limited exceptions. Therefore, the Directive will be the most important international regulation in the field of data protection in the European Union.

When drafting the Directive, the Commission had to look not only at international regulations but also at national laws in the Member States. Two countries (Italy and Greece) still do not have data protection legislation but all others do. Every country promoted its own idea of data protection in the decision-making process for the Directive. The Commission decided to create the Directive on a high standard, realizing that in some countries data protection had a constitutional impact. Thus, the Commission merged different systems together and the Directive provides a registration system, detailed provisions about the lawfulness of processing, sensitive data provisions, wide provisions for information to the subject and strong control rights. The Commission tried to implement all legal instruments it found in the present laws of Member States in order to secure a high level of protection. During the negotiations in the Council, the Directive allowed for different methods to ensure data protection in the Member States. In the final directive there are more choices for implementation and Member States may keep many of their existing laws.

Data protection regulations must provide exemptions from their rules in order to be applicable in practice. All international regulations and all national laws include exemptions. Exemptions are very impor-

237. Council Directive, *supra* note 1, arts. 29, 30.

tant in order to judge the effect of data protection regulations because wide exemptions will cripple the regulations. The Directive contains a large number of loopholes in two different ways: first, Member States are offered the possibility to provide special regulations like in Article 13; second, provisions like Article 7(f) provide exemptions directly for the controller. If a Member State uses all the possible loopholes to minimize the effect of the Directive and if users widely rely on general exemption clauses then the effect of the Directive might be considerably weakened.

The extent of derogation from the Directive is mainly a problem of interpretation of the regulation, because there is no common understanding of the Directive within Europe. Every country is likely to interpret the Directive based on its own legal background in data protection. One of the main differences is because in some countries data protection rights are based on the constitution. The U.K., for example, has no general privacy right while the German Constitutional Court has strongly enforced privacy. Especially in the interpretation of clauses balancing user and subject interests, such differences may cause gaps in the practical effect of the Directive in the Member States.

Based on the Directive, Member States must change their national laws. For example, the U.K. must make far-reaching modifications, because the U.K. system is basically a registration system, which does not provide detailed provisions for the lawfulness of processing of personal data. There are already attempts by the Registrar to create a stronger interpretation of the data protection principles, but, under the Directive, the U.K. legislature has to implement special provisions for the lawfulness of processing. Also, the requirements for consent and the provisions for information processing to the subject have to be changed. One important change will occur through to the extension of the Act on structured manual data. On the other hand, the English legislature might have the chance to limit the registration procedure. Compared with the U.K., the German system already provides strong and detailed provisions about the lawfulness of processing and information about a subject. The German Act also covers, in the public sector, manual data and a registration system. However, the private sector regulations must be changed under the Directive because they, to some extent, do not cover manual data and they do not have specific third country regulations. On the other hand, the German Act provides detailed provisions or sectoral provisions which might be stronger in their effect than the Directive. Therefore, the question arises whether this might cause trade obstacles in the future and whether the provisions have to be changed. Article 5 of the Directive provides the right of Member States to enact stronger regulations. However, since Article 1 (2) obliges the Member States to ensure the free flow of data, stronger regulations would be not allowed as an obstacle to free data flow.

The Directive has not only an impact on Member States but also impacts non member countries, like the U.S., that wish to transfer data to or from a European Union country. They must ensure an adequate level of protection if they want to exchange personal data. The third country regulations in the Directive raise the issue of whether there is adequate protection in a specific transaction. If third countries do not change their general law in order to provide adequate protection, it is debatable whether contractual regulations between partners of transactions are capable of meeting the requirements of the Directive.

The Directive is the most important international data protection regulation for the Member States of the European Union and will effect other countries that want to trade with Member States. Based on a human right understanding of privacy and freedom, the Directive establishes strong provisions for the protection of individuals against the risks of processing of personal data. On the other hand, unspecific exemption clauses and the range of possible interpretation of provisions might be used as loopholes to demolish the intent of the Directive. Therefore, a common interpretation of the Directive is needed. Such an interpretation must consider the historical roots of the Directive. A European Union-wide discussion of the Directive is needed and Member States have to be convinced that harmonised data protection is essential in the Community because otherwise, every problem would need to be solved by the European Court of Justice.