International Journal of Law and Information Technology, Vol. 1 No. 2 Summer

Information Management and Data Protection within the EC – the amended EC proposal for a council directive on data protection and its impact on German industry

THOMAS HOEREN[1]

1 Introduction

Information managers and lawyers have always followed conflicting principles for two main reasons:

1.1 New technology versus traditional law

The information technology market has expanded immensely during the last 20 years and has changed fundamentally all parts of social life. The second technological revolution created by the expanding use of computers stresses the antiquity of legal thinking. Lawyers use methodological

[1] Institut fur Kirchenrecht, University of Munster.

instruments that date from the 19th century, but have begun to feel that these instruments are going to be insufficient for solving the legal problems of the computer age.

This problem is especially reflected in the data protection area. The statutory regulations on data protection have always referred to a technological standard which has been overruled by the time the regulations have been enacted. This legal time lag may be exemplified by looking at the situation in Germany.

Germany has a very old tradition of protecting personal data. The German state of Hessen enacted the world's first data protection Act in 1970.[2] This Act was mainly influenced by the decision of the Federal Constitutional Court of July 1969 stating that the protection of privacy is guaranteed as part of the German constitution.[3]

However it took seven years (1970-1977) to develop a Federal Data Protection Act (Bundesdatenschutzgesetz BDSG).[4] This Act entered into force on 1 January 1978. On the basis of these regulations, all German states created data protection statutes and installed supervisory authorities by 1981. However, these state Acts did not contain any regulation on personal computers, computer networks, databases or transborder data flow. Instead they related to non-automated files and the big mainframe computers used by government and major businesses.

The situation changed totally with the decision of the Federal Supreme Court of 15 December 1983 dealing with the constitutionality of the 'microcensus' (the 'Volkszählungsurteil').[5] The court expressly referred to the fact that the existing regulations on data protection did not reflect the increasing use of computers. Thus, they postulated several constitutional principles which would protect the privacy of individuals in the computer age. In particular, the judges held that

- each citizen has a right to decide if and where his personal data should be used (the right to informational self-determination/ 'Recht auf informationelle Selbstbestimmung');
- this fundamental right can only be limited with the express consent of the person concerned or by detailed statutory regulation;
- all personal data is to be protected irrespective of its sensitivity;
- each citizen must be informed who is using his data, which data are used and where and when they are used;

---

[2] Gesetzes-und Verordnungsblatt 1970 I, p. 625.

[3] Decision of 16 July 1969 – 1 BvL 19/63 = BVerfGE 27, 1; cf. the decision of the Court of 15 January 1970 – 1 BvR 13/68 = BVerfGE 27, 344 = NJW 1970, 555.

[4] *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27.1.1977 – Bundesdatenschutzgesetz* Bundesgesetzblatt 1977, I, 201.

[5] Decision of 15 December 1983 – 1 BvR 209/83 = BVerfGE 65, 1 = Neue Juristische Wochenschrift 1984, p. 419.

- personal data can only be used and transferred for a specific purpose, so that the collection of data so as to hold a potentially useful 'stock' of information is always unlawful.

These rigorous principles of data protection have been integrated into a new Federal data protection Act which entered into force on 1 June 1991.[6] This Act expressly refers to personal computers and online facilities. But unfortunately, it does not deal with transborder data flows.

1.2 International networks versus national jurisdiction

Information management is not limited by national frontiers. The exchange of data and the establishment of networks have always taken place irrespective of national borders. Although this aspect might be fortunate for the information industry, it is dangerous from the viewpoint of lawyers. Law is in general national, created by national legislators and enforced by national courts and authorities.

The difficulties raised by international computer networks are in particular manifested by transborder data flows. This phenomenon has always been one of the central problems of data protection; in an era of multinational networks it is possible to transfer data of a German enterprise to an Italian Rechenzentrum without any delay.

This possibility may be used by enterprises to circumvent national data protection legislation. If an enterprise disapproves of a national data protection Act and the corresponding state control, it may carry out its computer operations from foreign territories. All important personal data (especially those of employees and customers) will be stored in a foreign data processing centre from where they could be transferred anywhere in the world.

Up to now, the international regulations on this topic have not succeeded in dealing with transborder data flows[7]:

---

[6] Bundesgesetzblatt 1990 I, 2954. There are a number of commentaries and handbooks which have been published with regard to the new statute. See for instance Auernhammer, *Bundesdatenschutzgesetz* Cologne 1991; Bergmann/Möhrle/Herb, *Datenschutzrecht, Handkommentar* Stuttgart (Looseleaf) September 1991; Dörr/Schmidt, *Neues Bundesdatenschutzgesetz. Handkommentar* 2nd. ed. Cologne 1992; Gola/Wronka, *Handbuch zum Arbeitnehmerdatenschutz* Cologne 1989; Ordemann/Schomerus, *Bundesdatenschutzgesetz* 5th ed. Munich 1992; Tinnefeld/Ehmann, *Einführung in das Datenschutzrecht* Munich 1992; Wohlgemuth, *Datenschutzrecht. Eine Einführung mit praktischen Fällen* Neuwied 1992.

The best commentary is by Simitis/Dammann/Geiger/Mallmann/Reh, *Kommentar zum Bundesdatenschutzgesetz* Baden-Baden (Looseleaf) January 1992.

[7] For the international aspects of data protection cf. Mengel, *Internationale Organisationen und transnationaler Datenschutz* Berlin 1984; Wochner, *Der Persönlichkeitsschutz im grenzüberschreitenden Datenverkehr* Zürich 1981; Simitis/Dammann/Geiger/Mallmann/Walz, op. cit. Note 6 above, ¶ 1 Note 108 et seq.

- The recommendation of the OECD of 23 September 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data[8] is not legally binding and is too abstract.[9]
- The same problem arises with regard to the guidelines of the United Nations concerning computerised personal data of 4 December 1990.[10]
- The Convention of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data has been implemented in Germany.[11] However, it only contains general principles that might be enacted in different ways. In addition, the treaty has only been ratified by seven member states.

Restrictions on transborder data flows also endanger the development of a uniform European common market: up to now, only nine EC member states have enacted regulations on data protection (Germany, Denmark, France, Ireland, Portugal, Luxembourg, Netherlands, Spain and Great Britain). The other member states have no specific data protection legislation. This leads to dangerous data havens within Europe; in the south of Europe (and in Belgium) the processing of personal data is allowed without any legal limitations, by contrast with the north of Europe where detailed control mechanisms have been developed.

2 Activities of the EC[12]

The EC had to be active in this area. The European Parliament adopted several resolutions in 1976[13] asking the EC Commission for an EC data pro-

---

[8] Reprinted in Chalton/Gaskill (Eds.), *Encyclopedia of Data Protection* London 1993, No. 7-223. German version published in *Bundesanzeiger Amtlicher Teil* Nr. 33/215 vom 14 November 1981.

[9] See Ellger, *Datenschutz im grenzüberschreitenden Datenverkehr – eine rechtsvergleichende und kollisionsrechtliche Untersuchung* Baden-Baden 1990, 520 ff.; Bothe/Kilian, *Rechtsfragen grenzüberschreitender Datenflüsse* Cologne 1992, 552 ff.; Siepel, *Transborder Flows of Personal Data. Reflections on the OECD Guidelines* TDR 1981, 32 et seq.

[10] See Simitis/Dammann, op. cit. Note 6 above, ¶ 1 Note 148; Ellger, op. cit. at Note 9 above, 564 ff.

[11] *Bundesgesetzblatt* 1985 II, 539. Cf. Henke, *Die Datenschutzkonvention des Europarats* Berlin 1986; Schweizer, *Die Konvention des Europarats und die Richtlinien der OECD zum internationalen Datenschutz aus schweizerischer Sicht* Informatique et protection de la personnalité 1981, 255 et seq.

[12] Cf. Ellger, *Datenschutz und europäischer Binnenmarkt* Recht der Datenverarbeitung 1991, 57 et seq. and 121 et seq.; Koch, *Rechtsvereinheitlichung und Kollisionsrecht im Recht des grenzüberschreitenden Datenverkehrs – Europäische Initiativen* Recht der Datenverarbeitung 1991, p. 105 et seq.; Papapavlou, *Überlegungen der EG-Kommission zum Datenschutz im Informationsdienstleistungssektor* Recht der Datenverarbeitung 1990, 113 – 116; Riegel, *Europäische Gemeinschaften und Datenschutz* Zeitschrift für Rechtspolitik 1990, 132 et seq.; Schneider, *Die EG-Richtlinie zum Datenschutz* Computer und Recht 1993, 35 – 40; Spannowsky, *Deutscher Datenschutz und Datenschutz der EG* in: REDP/ ERPL 3 (1991), 31 – 45; Wind/ Siegert, *Entwurf für eine EG-Richtlinie zum Datenschutz* Computer und Recht 1993, 46 – 55.

[13] OJ C 60/48 of 13 March 1975; OJ C 100/27 of 3 May 1976; cf. OJ C 140/34 of 5 June 1979; OJ C 87/39 of 5 April 1982.

tection directive.[14] The Commission was not very quick to respond to this demand; it was 14 years before they published a collection of regulations on the question of data protection on 18 July 1990.[15] The package includes among others:

- The 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.
- The proposal for a council directive on the protection of personal data in the telecommunications sector.

These proposals have been sent to the Economic and Social Committee which delivered its opinion on the proposals on 24 April 1991.[16] On 11 March 1992, the European Parliament approved a number of amendments proposed by the Committee of Legal Affairs and Citizens' Rights.[17] As a consequence, the EC Commission published an amended proposal on 15 October 1992.[18] It is not yet known when this amended proposal will be decided upon by the Council of Ministers.

The directive will lead to many changes in the national legislation of each member state. This article will attempt to demonstrate the possible consequences of the directive for private industry, with special focus on the situation in Germany. Although the author is from Germany, the German example has not been chosen for the purpose of nationalism. As demonstrated below, Germany has enacted the most restrictive data protection legislation in the world. It is therefore instructive to examine the changes which will result from the EC directive from a German perspective.[19] It is not possible to discuss all aspects of the directive. Instead some major elements will be presented which are of great importance for an industrial view.

3 Details of the directive

3.1 Equalisation of the private and public sector

The German Federal Data Protection Act makes a strict distinction between the private and the public sector. While all personal data stored or

---

[14] Cf. H. Meister, *Europäische Harmonisierung des Datenschutzes* in: Datenschutz und Datensicherung 1980, p. 9 et seq.

[15] COM (90) 314 fin. – SYN 287 = OJ C 277/3 of 5 November 1990.

[16] OJ C of 17 June 1991.

[17] Document A3 – 0010/92, Doc. EP 160.503.

[18] COM (92) 422 final – SYN 287 = OJ C 311/30 of 27 November 1992.

[19] This German focus is the reason, too, for quoting (almost) exclusively German literature in this article. For the international view on the EC directive cf. Nugter, *Transborder Flow of Personal Data within the EC – A Comparative Analysis of Germany, France, the United Kingdom and The Netherlands and their Impact on the Private Sector* 1990.

used within the private sector are protected, the Act only applies to the private sector where personal data are stored within a file (automated or non-automated). In addition, private and public data processing are dealt with in different parts of the Federal Data Protection Act; some aspects of the public sector have even been regulated by specific Acts (such as social security or police Acts).

For this reason, German lawyers have to decide in advance whether an institution is part of the private or public sector. As in Great Britain,[20] this decision is very complicated and difficult. For instance, the classification of religious groups is a matter of some controversy.[21]

This situation will however be changed by the EC directive. The initial proposal had distinguished between the processing of private and public organisations. In the new proposal the sectors have been mingled. This new concept does not facilitate the readability and understanding of the directive. For instance, art. 13(5) provides that each data subject has to be informed of the reasoning applied in any automatic processing operations (whatever that means) the outcome of which is invoked against him. This right of the data subject which originally referred to automated acts of administration, now applies to the private sector too. In the case of a contract concluded using on-line facilities, the data subject has thus to be informed of the reasons for any refusal to enter into a contract.

3.2 Applicability

According to Sect. 3(1), the Federal Data Protection Act only protects specific data of an identified or at least identifiable individual. Thus the data of legal persons are not protected under the Act (unlike in Luxembourg, Denmark, Austria and some other European states).

In the same way, the directive applies to all information relating to an identified or identifiable natural person (art. 2(a)). The data of legal persons are not protected. The protection of data is restricted to personal data processed by automatic means within a file (art. 3(1)). This restriction to files is contradictory to the proposals of the European parliament and to German law, which extends the protection to non-structured records held by the public sector.

3.3 Lawfulness of processing

According to the Federal Data Protection Act, as a general principle the

---

[20] Cf. Beatson, *Public and Private in English Administrative Law* [1987] LQR 34 et seq.

[21] Cf. Hœren, *Kirchen und Datenschutz. Kanonistische und staatskirchenrechtliche Probleme der automatisierten Datenverarbeitung* Essen 1987; Lorenz, *Die Stellung der Kirchen nach dem Bundesdatenschutzgesetz 1990* Zeitschrift für evangelisches Kirchenrecht 37 (1992), 27 et seq.; Dammann, *Die Anwendung des neuen Bundesdatenschutzgesetzes auf die öffentlich-rechtlichen Religionsgesellschaften* Neue Zeitschrift für Verwaltungsrecht 1992, 1447 et seq.; Hoeren, *Kirchen und das neue BDSG – Zugleich eine kritische Erwiderung auf Dammann* NVwZ 1992, 147 ff., *Neue Zeitschrift für Verwaltungsrecht* 1993 (to be published soon).

processing or use of personal data, whether in or out of files, is forbidden in the private sector. The same applies to the public sector even if the data are held in unstructured records. As an exception, data processing is lawful:

- where the person concerned has consented in writing;
- where there is an agreement between a works council (or trade union) and management[22]; or
- where processing is permitted by a detailed statutory order or permission.

Some statutory provisions permitting data processing have been integrated in the Federal Data Protection Act. According to Sect. 28, personal data may be processed or used in the private sector:

- if these acts are necessary for the discharge of a contract or a quasi-contractual relationship of trust (for instance in the course of employment or banking contracts);
- if processing is necessary for the realisation of lawful interests of the user unless the person concerned has a prevailing interest in preventing the use (such as in the case of medical or criminal data);
- if the data come from sources generally accessible to the public (e.g. telephone books, television news, public registers);
- if the data are used for scientific research and they will be 'anonymised' as soon as possible.[23]

The German concept has obviously been adopted by the EC Commission. According to art. 7 personal data may be processed in the private sector only if:

- the data subject has consented (art. 7(a)); or
- the processing is necessary for the performance of a contract with the data subject or in order to take steps at the request of the data subject preliminary to entering into a contract (art. 7(b)); or
- the processing is necessary in pursuit of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject (art. 7(f)).

---

[22] Decision of the Federal Labour Court of 27 May 1986 – 1 ABR 48/84 = Betriebs-Berater 1986, 1087 = Neue Juristische Wochenschrift 1987, 674; Judgment of the Court of Appeal of Düsseldorf of 4 November 1988 – 17 (6) TaBV 114/88 = Recht der Datenverarbeitung 1989, 243, 247 = Neue Zeitschrift für Arbeitsrecht 1989, 146, 147.

These decisions have been criticised by literature as being contradictory to the BDSG; cf. Hoeren, *German data protection law*, in: Keustermans/Arckens (eds.), *International computer law*, New York 1993 (forthcoming).

[23] Cf. sect. 40(3). For the privileges of science with regard to data protection cf. Bizer, *Forschungsfreiheit und informationelle Selbstbestimmung* Baden-Baden 1992.

However some other provisions of the Federal Data Protection Act have not been integrated in Art. 7. For instance the public register provision mentioned above had been part of the first proposal (art. 8(1)(b)) but is omitted in the amended version. Furthermore, the use of personal data for scientific research has not been regulated in the proposal; perhaps the provision on the legitimate interests of the controller (art. 7 (f)) could be applied here.

3.4 Sensitive data

The German data protection law is characterised by the protection of all personal data. The Constitutional Court has always held that there is no distinction between personal data which are seemingly sensitive and those which are not. The Court expressly stated that there is a state obligation to protect any personal data irrespective of their sensitivity. The legislator has fulfilled this obligation in the Federal Data Protection Act by protecting all personal data to the same extent. Only sect. 28(2) refers to the idea of different spheres of protection by permitting the transmission of some non-sensitive data to third persons.

In contrast to German law, the directive has decided to apply the French idea of sensitive data. Art. 8 provides that any processing of personal data revealing:

- racial or ethnic origin,
- political opinions,
- religious beliefs,
- philosophical or ethical persuasions,
- trade union membership, or
- health or sexual life

is generally forbidden. However, art. 8(2) allows such processing under certain circumstances. Religious groups may for instance use such data in the course of their legitimate activities (art. 8(2)(b)). This regulation implies that religious organisations will in fact be obliged to obey the directive (i.e. the national Act implementing the directive). This is really a new aspect for German lawyers which raises controversy about the classification of churches in data protection law. The churches have always taken the view that they are not bound by data protection laws; they will have to change their attitude after the implementation of the directive.

In addition, the processing of sensitive personal data is allowed where the data subject has given his written consent to the processing (art. 8(2)(a)) or where the processing is performed in circumstances where there is manifestly no infringement of privacy or fundamental freedoms (art. 8(2)(c)).

This last exemption is vague and abstract. It is in particular strange that only a 'manifest' infringement of fundamental freedoms should prohibit the processing of sensitive data. Furthermore, the distinction between privacy fundamental freedoms causes some problems of understand-

ing: Is the right to privacy not a fundamental freedom? What is meant by 'privacy' then? Does this wording refer to the American concept of different categories of personal data[24] (which contrasts with the principles of German constitutional law referred to above)?[25]

In addition, art. 17(3) of the initial proposal prohibited any data processing concerning criminal convictions in the private sector. This regulation proved to be too rigid; in many cases private organisations need data on criminal convictions (e.g. those granting credit). The amended proposal repeats the prohibition in art. 8(4), but member states are allowed to lay down exemptions from this rule. Of course, Germany will use this possibility.

3.5 The private data protection commissioner

The German legislator has decided in the Federal Data Protection Act to support a self-regulatory control system with regard to data protection. All enterprises have to appoint and pay for an independent data protection commissioner who is responsible for the control of data protection within the enterprise (sect. 36). The commissioner is responsible for any data protection issues in the enterprise (apart from those involving the works council). There are some supervisory authorities, too, mentioned in the Federal Data Protection Act. These only control the qualifications of the private data protection commissioner (sect. 36(3)) and have powers to assist him if he has problems with the management (sect. 37(1)). The public authorities are not themselves allowed to control data protection in the enterprise on a regular basis (sect. 38(1)).

This system, which may be regarded as strange from a foreign viewpoint, has in fact been very efficient. Most of the commissioners have regarded their tasks as important and responsible, although the qualifications of many commissioners have been weak.

However, the directive will abolish this system. The German data protection organisations noticed too late that the directive does not provide for a self-regulatory control institution. Instead Art. 30 provides that each member state shall designate an independent *public* authority to supervise the protection of personal data. This regulation is influenced by the idea that state control is the only way to supervise data protection.

German practitioners are now vehemently discussing the future of the data protection commissioner.[26] The obligation of enterprises to appoint a commissioner will of course have to be abolished. Corporations may

---

[24] Cf. Wacks, *The Protection of Privacy* London 1980; Pratt, *The Warren and Brandeis Argument for a Right to Privacy* in: Public Law 1975, 161 et seq.; Prosser, *Privacy* California Law Review 1960, 38 ff.

[25] For the German view see Steinmüller et al., *Grundfragen des Datenschutzes. Gutachten im Auftrage des Bundesministerium des Inneren* Bundestagsdrucksache 6/3826 vom 7 September 1972, 51 et seq.

[26] Geis, *Die europäische Perspektive des betrieblichen Datenschutzbeauftragten* Computer und Recht 1993, 31 et seq.

appoint a commissioner if they want, but they will not want to have an independent control institution within the enterprise in addition to the public authorities.

3.6 Notification

Great Britain has been the origin of another element of the proposal which will cause a lot of problems from a German perspective: the obligation to notify.[27]

According to sect. 32 of the Federal Data Protection Act, only organisations which mainly deal with the transfer of data are obliged to notify some aspects of their processing to the supervisory authorities. The situation is different in the UK where the Data Protection Act 1984 provides for extensive obligations to register with the Data Protection Registrar (c.f. Sects. 4-9 of that Act). However, it is not known in Germany whether the concept of registration is regarded as sufficient and effective in Britain.

Nevertheless, the British concept has been integrated in the proposal. Art. 18 provides that the controller of a file must notify to the supervisory authority before carrying out processing at least:

- the name and address of the controller and of his representative;
- the purpose of the processing;
- the categories of data subject;
- a description of the types of data to be processed;
- the third parties to whom the data might be disclosed;
- any intended transfers of data to third countries;
- a description of the measures which ensure security of processing;
- any change to the information listed above.

Only certain non-sensitive categories of processing may be exempted from this obligation (art. 19), such as the production of correspondence or the consultation of documentation services accessible to the public.

These regulations are a nightmare for German industry. It has been estimated that the 100 biggest enterprises in Germany will have to perform 300,000 notifications per month because of the directive.[28] This estimate may be exaggerated, but it demonstrates the German fear of being part of a bureaucratic notification system.

3.7 Problems of private international law

The Federal Data Protection Act provides that all data users domiciled in Germany are obliged to observe its provisions (cf. Sect.27(1) and Sect.

---

[27] A second British element consists of the 'principles relating to data quality' (art. 7). From a German perspective, these principles are irrelevant because they are a matter of course and thus need not be expressly regulated in a directive.

[28] This is the result of a study of the 'Gesellschaft für Datenschutz und Datensicherung' (Society for data protection and security/GDD); cf. GDD, *Mitteilungen 1992* Heft 5/6, p. 10.

2(4)).[29] Hence the German law has to be applied if a data user, i.e. the person storing or transferring personal data, has its domicile, i.e. its usual residence or seat,[30] in Germany.

This is the reason why the Federal Data Protection Act applies irrespective of the nationality of the data subject. Every data subject who is affected by data processing of a German file controller is able to use his rights under the Federal Data Protection Act, independent of his nationality.

The EC Commission has had some problems in solving the private international law issues involved in data protection. Art. 4 of the initial proposal stated that each member state was to apply the directive to all files located in its territory or to the controller of a file resident in its territory. This regulation would lead to a peculiar situation. If an American owner of a notebook computer storing the personal data of American citizens entered the territory of a member state, its national law would apply irrespective of the fact that the persons concerned and the file controller were Americans.

For this reason the amended proposal has changed the regulation. Now the national provisions have to be applied to all processing of personal data of which the 'controller' is established in its territory. The term 'controller' is yet not identical with the German data 'user'. According to Art. 2 (d), 'controller' means every person who:

- processes personal data or causes it to be processed; *and*
- who decides what is the purpose of processing, which operations are to be performed upon the data and which third parties are to have access to them.

The EC directive thus stresses the element of control while the German concept refers to the processing of personal data. It will however be very difficult to determine the 'controller' of a file. Multinational corporations have a very complex structure with regard to information management; an American headquarters may for instance determine the organisation of IT within its European subsidiaries.

The EC Commission tried to deal with the problem partly by extending the scope of applicable national law. According to Art. 4(1) (b) the member states have to apply their national provisions to all processing of personal data by a foreign controller where 'he makes use of means which are located in the territory of that Member State'. This regulation is very unclear as to the term 'means ... located in the territory'. The Commission stated that this regulation is related to the use of 'terminals, questionnaires

---

[29] See Ellger, op. cit Note 9 above, p. 604 et seq.

[30] See the decision of the Federal Supreme Court of 5 November 1980, BGHZ 78, p. 318, at p. 334; Großfeld, *Praxis des Internationalen Privat- und Wirtschaftsrechts* Reinbek 1975, p. 44 et seq. The German definition of the domicile of corporations is different from the definition in England; cf. *Ceena Sulphur Co. Ltd. v. Nicholson* (1976) 1 Ex. D. 428; *De Beers Consolidated Ltd. v. Howe* (1906) A.C. 455; *Swedish Central Ry. v. Thompson* (1925) A.C. 495.

etc.'.[31] But when does a foreigner 'make use' of these means? Is national law applicable even where:

- a foreigner uses a notebook computer in a EC Member State (see above)?
- he is using online and telecommunication facilities?

3.8 Transborder data flows

The Federal Data Protection Act does not contain a specific regulation on the export of data. The legislator has refused to create new provisions on transborder data flows although many commentators have criticised this statutory gap.[32]

It is 'opinio communis' in Germany that personal data may never be transferred into foreign states which have not implemented an equivalent standard of data protection.[33] But what is meant by 'equivalence'?[34] Which states are provided with a data protection law comparable to the (very high) German standard? From a German perspective the US regulations on data protection are very insufficient and inadequate.[35] It has recently even been supposed that no state in the world really has a standard of data protection comparable to Germany.[36] This would lead to Germany becoming an isolated fortress of data protection unable to communicate with foreigners. This danger is further increased by the view of academic literature that international contracts on data protection cannot ensure an equivalent level of protection.[37]

The problem has been made worse by the proposed EC directive. According to Art. 26 of the proposal the transfer of personal data to non-EC countries will only be lawful if those countries ensure 'an adequate level of protection'. But what is meant by 'adequate level of protection'? Does this term refer to the EC standard of protection or to the national data protection regulations of an EC member state? The member states will in fact have different data protection laws even after the implementation of the direc-

---

[31] Amended Proposal, COM (92) 622 final – SYN 287, p. 13.

[32] See Simitis/Dammann, *Bundesdatenschutzgesetz* 3rd ed. Baden-Baden 1981, ¶ 22 Note 51; Simitis, *Grenzüberschreitender Datenaustausch – Notwendige Vorbemerkungen zu einer dringend erforderlichen Regelung* Festschrift für Murad Ferid zum 70. Geburtstag, Munich 1978, p. 354 – 375.

[33] Cf. Simitis/Dammann/Geiger/Mallmann/Walz, op. cit. at Note 6 above, ¶ 1 Rdnr. 93 with further references.

[34] For this difficult problem see Riegel, *Gemeinschaftsrechtlicher Datenschutz. Entwurf einer EG-Datenschutzrichtlinie* Computer und Recht 1991, p. 181; Simitis, *Datenschutz und Europäische Gemeinschaft* Recht der Datenverarbeitung 1990, p. 11.

[35] See Tinnefeld, *Der Datenschutz in den Vereingten Staaten – Die gegenwärtige Situation* Recht der Datenverarbeitung 1992, p. 216 et seq.

[36] Hoeren, *Electronic Data Interchange: The Perspectives of Private International Law and Data Protection* in: Law, Computers and Artificial Intelligence Vol. 1.3 (1993) 329.

[37] Cf. Simitis/Dammann, *BDSG*, 3rd. ed. Baden-Baden (Nomos) 1981, ¶ 22 Note 55; this view has recently been rejected by the Data Protection State Commissioner of Hamburg in his 10th Report of November 1990, p. 105.

tive because the directive leaves a lot of questions to be solved differently by the member states.[38] It has thus to be defined whether 'adequacy' refers to a national or a European standard of data protection.

Art. 26(1) provides, too, some exceptions where personal data may be transferred to a non-EC state with inadequate data protection. In the private sector the proposed transfer will be lawful

- if the data subject has consented to the transfer in order to take steps preliminary to entering into a contract; or
- the transfer is necessary for the performance of a contract between the data subject and the controller and the data subject has been informed of the inadequacy of data protection law in that country.

These exceptions are difficult to understand. The consent of the data subject should be required to legitimate a transfer in every case, not merely before closing a contract. Imagine a person entering a travel office in the EC in order to book a hotel room in Fiji. It may be supposed that Fiji has no adequate data protection law. According to the directive, the travel office is not allowed to transfer the data of the customer to the hotel in Fiji. As an exception, the office may perform the reservation if the customer has given his (written and express) consent prior to the closing of the travel contract. If the office has forgotten to ask for consent, the data subject is not allowed to give his consent afterwards. Instead he has to be informed by the travel office that Fiji has no adequate level of protection. Then and only then may his data be transferred for making the hotel reservation.

This concept contradicts the idea of self-determination. The data subject is the one who has to decide about the future of 'his' data. If he consents to a transfer of data, the transfer must be lawful in any case. The EC Commission is simply patronising the data subject against his express will. It is not understandable why the Commission has not implemented the proposal of the European Parliament that transborder data flows should always be lawful where there is an express consent of the data subject.[39]

Furthermore, the proposal presumes that contractual arrangements between the controller and members of third countries on transborder data flows and data protection are in general invalid if the third country has no adequate level of protection. The proposal exceptionally accepts transborder data flows contracts under special conditions (Art. 27):

- First, the controller of the file has to give sufficient justification that an adequate level of protection will be provided.
- Secondly, the Member state in which the controller has its residence has to authorise such a transfer of data.

---

[38] See in particular arts. 5, 8(3), 9, 10(2), 14(1), 14(3), 18(5), 20, 23(2), 28 et al.

[39] Cf. No. 78 and 127 of the amendments adopted by the European Parliament on 11 March 1992: 'The transfer of personal data to a third country may require the express consent of the data subject'.

- Finally, the EC commission and all member states have to be informed in good time so that notice of opposition may be given.

On the one hand, this procedure is too bureaucratic and cumbersome. On the assumption that the United States has a low standard of data protection compared to Europe, the transfer of any personal data from Europe to the United States will be subject to a complicated system of control and authorisation. This system includes any transfer notwithstanding its importance and extent and even within an international combine; thus it may threaten worldwide scientific and technical co-operation and will cause a lot of problems for international corporations.

On the other hand, it remains unclear how a controller of a file should guarantee an adequate level of protection by means of a contract. This contract must be drafted as a contract between the controller and the transferee in favour of a third person (i.e. data subject). This way of drafting runs counter to the doctrine of 'privity of contract' which is part of English law tradition. In Germany it is possible to draft a contract in that way, but this construction has led to a lot of difficult legal problems which have not been solved up to now. For instance, it is doubtful whether the contract may be terminated by the controller or transferee without the consent of the data subject.[40]

4 Conclusion

The proposed EC Directive is a strange mixture of three different models of data protection:

- It implements the German idea of prohibiting any processing of personal data except where there is a written consent or a statutory permission (Art. 7).
- In addition, the French idea of special protection for sensitive data is integrated into the proposal (art. 8).
- Finally, the British stress on notification has found its European expression in arts. 18 and 19 of the proposal.

These three models had already been introduced in the initial proposal; in the amended version the rigidity of the models has been reduced by granting national derogations. But the second proposal is still suffering under the inconsistency of the British, French and German features mingled

[40] For further problems see Hoeren, op. cit. at Note 36 above. The Council of Europe has tried to solve these problems in its 'Model Contract' published on 2 November 1992 (T-PD (92) 7 revised). This expressly gives the licensor (transferee) the right to terminate irrespective of the data subject's consent.

together. Industry will be unduly burdened by the obligation to comply with the data protection requirements of three nations.

It is small wonder that German industry has strongly rejected the plans of the EC Commission. According to an opinion poll made last November,[41] 90% of 110 corporations believed that the EC directive would have no positive effects on the establishment of the single European market. Most of them were afraid of the high administrative costs.

Even the Federal Data Protection Commissioner, Dr. Alfred Einwag, has stressed at a conference in Munich on January 30 1992 that the EC directive will only establish a minimum regime of data protection. In his opinion the EC member states will still be allowed to create more restrictive data protection regulations; therefore, Germany need not change its legislation because of the directive.

I do not agree with this way of thinking. Art. 1(2) of the EC proposal expressly states that the member states 'shall neither restrict nor prohibit the free flow of personal data between Member States' with regard to their national data protection law. Any regulation on data protection which goes beyond the scope of an EC directive will become an obstacle to the free flow of data within the Community.

Therefore, the German authorities would violate Art. 8a of the EC treaty and the idea of an European market without frontiers by postulating national regulations on transborder data flows different from the EC directive. The efforts of the EC Commission to establish a uniform level of data protection within Europe will force the German legislator to adopt the EC regulations and change the German Data Protection Act fundamentally. As well as other EC member states, Germany will have to abolish its constitutional vision of data protection in favour of economic progress.

[41] Gesellschaft für Datenschutz und Datensicherung (ed.), *Auswertung der Erhebung überdie möglichen Auswirkungen der geplanten EG-Datenschutzrichtlinie auf die Wirtschaft.* Vorgelegt zur 16. DAFTA am 12. bis 13 November 1992 in Köln, Cologne 1993, p. 10.