Law, Computers & Artificial Intelligence, Volume 1, Number 3, 1992

Electronic Data Interchange: the perspectives of private international law and data protection [1]

THOMAS HOEREN
Institut für Kirchenrecht, Münster, Germany

ABSTRACT The following considerations deal with the impact of private international law and data protection regulations on electronic data interchange (EDI). The article is based on the example of a German corporation which transfers personal data of employees to a British transferee. These transborder data flows lead to the difficult question of which law has to be applied. It is intended to show that the regulations of the German Data Protection Act (BDSG) have to be applied in this case. A contractual choice of law is invalid because of the mandatory nature of the BDSG. According to the German act, personal data can only be transferred to foreign states with an equivalent legislation on data protection. A comparison between the British and the German regulations shows that the British law is not likely to be equivalent to the German standard. Therefore, it is very doubtful whether personal data are allowed to be transferred from Germany to Great Britain. The transferor and transferee may, however, make some contractual arrangements on data protection (especially on the rights of the data subjects to access and rectification); if the contract has been carefully drafted with respect to this item, a transfer of data may be regarded as lawful. The difficult problems demonstrated in the article show that further developments in EDI may be restricted and prevented by data protection and private international law; the EEC authorities will have to deal with these problems quickly and more effectively before the establishment of the European Single Market in 1993.

Who steals my purse, steals trash; 'tis something, nothing;
'Twas mine, 'tis his, and has been slave to thousands;
But he that filches from me my good name
Robs me of that
Which not enriches him
And makes me poor indeed.
(Othello: Act 3, Scene 3)

The increasing use of electronic data interchange (EDI) leads to many difficult problems in data protection law which have practically not been considered by court and academic literature up to now. Millions of sensitive personal data may be transferred daily from one country to another with the aid of EDI.[2] Data subjects have a right to be protected against these transborder data flows (TBDF), especially when their data are transferred to countries with inadequate data protection law.[3] However, almost all data protection acts in the world have the taint of administrative law and consequently, only referring to national data transfers.[4] Additionally, the adaptation of data protection law to transborder data flows has been widely criticised as a "bureaucratic nightmare, impossibly cumbersome, ineffective".[5]

It is my aim to demonstrate how data protection law may be used as an effective weapon against national 'data havens' – without becoming a bureaucratic nightmare. Since it is not possible to refer to all data protection acts, I will restrict my remarks to an exemplary case:

A German company has decided to cooperate with a British company. They made an agreement that they use EDI for all relevant data exchanges. In particular, personal data of employees are going to be exchanged between the companies. The contract includes provisions for the rights of the employees to access and rectification of their data. The employees of both companies consider this contract and the transfer of data to be unlawful; the question comes before a German court.

EDI, Data Protection and the Question of Private International Law

First the question of what law is applicable in this case has to be discussed. Is this transborder data flow governed by German or British data protection law? Many theories have been discussed to solve this problem.[6] According to Rigaux, [7] the law of the state in which the data subject usually lives has to be applied. Some authors [8] regard the place of data processing (whatever that means) to be relevant; in a similar way, the EEC proposal for a Council directive on data protection [9] provides in Article 4(1)(a) that the directive has to be applied to "all files located in its territory". Finally, the use of the domicile of the data

users as a criterion for determining the relevant law has also been discussed.[10]

In my opinion, the discussion has been too unbalanced and narrow-minded. A distinction needs to be made between at least two different questions:

- Which law is generally applicable in transborder data flow issues?
- Which law is governing the contract on EDI and international data traffic?

The following considerations presume that these questions have to be solved with the aid of the German private international law; for each court uses its own national rules for the conflict of laws.

The General View

The first question is what law is generally applicable to transborder data flow issues. In Germany, this question is regulated by the new Data Protection Act of 20 December, 1990 (Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes/BDSG).[11] This Act does not contain a special provision on transborder data flows between private institutions.[12] However, the Act implies that all data users domiciled in Germany are obliged to observe its provisions (cf. sections 27(1) and 2(4)).[13] Hence the German law has to be applied if

- a data user, e.g. the person storing or transferring personal data,[14]
- has its domicile, e.g. his usual residence or seat [15], in Germany.

This is the reason why the BDSG does not differentiate according to 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 BDSG – independent of his nationality. In our example, the parties have agreed to exchange data mutually. Therefore, the transfer of data from Germany to Britain is governed by German data protection law because the transferring person has its seat in Germany. Inasmuch as the British company is transferring data from Britain to Germany, the transfer is governed by British law.

The Proper Law of a Contract on EDI

A different approach may be necessary to find the relevant law for a contract on EDI.

General rules of the lex contractus. The question of the law applicable to contractual regulations on EDI is governed by Articles 27-37 of the Einfuhrungsgesetz zum Burgerlichen Gesetzbuch (EGBGB). According to Article 27 EGBGB, the parties of a contract are free to choose the applicable law. If the parties have not made a selection (either explicitly or implicitly), the law that is most closely connected with the

contract must be considered (Article 28(1) EGBGB). This depends on the characteristic duties of the contract, especially on the main non-pecuniary obligation.[16]

The mandatory nature of German data protection law. These rules must not, however, be applied to contracts on EDI as far as personal data are concerned. According to Article 34 of the EGBGB, mandatory regulations continue to apply notwithstanding the parties' choice of a different law. The regulations of the BDSG are mandatory: [17] section 43 of the BDSG states that it is criminal to use data contrary to the BDSG. According to section 38 of the BDSG, the data protection authorities have to control the realisation of the provisions of the act; they are allowed to put heavy sanctions on the data users in the case of violations of the BDSG. Therefore, it is not possible to derogate from the regulations of the BDSG by contract. All disputes between the parties of the contract have, thus, to be settled by applying the law of the state in which the data user has taken his seat or residence (see above).

Application of the mandatory British data protection law? The final question is whether the mandatory British data protection law has to be applied beside the German law. Some authors suppose that mandatory foreign regulations on data protection should be applied under certain circumstances.[18] The German courts, however, have unanimously held that foreign law should never be applied if a contract is governed by German law.[19] In my opinion, this consideration has to be supported for the following reasons. The sovereignty of a state is restricted to its territory. National law is therefore only mandatory within the borders of a state; it loses its mandatory nature after 'leaving' the orbit of statual power. Consequently, it is not the task of German courts to enforce foreign 'mandatory' law in a case where German law applies. This legal situation has not been changed by the European Contracts Convention [20]; although Article 7(a) of the Convention permits the court to give effect to the mandatory regulations of some third country, the German legislator has reserved its right under Article 22(1)(a) not to apply Article 7(a).[21]

Summary

The German Data Protection Act is applicable in all cases of transborder data flow initiated by a person with seat or residence in Germany; foreign mandatory regulations have no effect in these cases. British law has to be applied where personal data are transferred from Britain to Germany. These rules are mandatory; a contractual choice of law is invalid (Article 34 EGBGB).

EDI and the New German Data Protection Act

Special Regulations

While Sweden, Denmark, Austria, Great Britain and France have included provisions on transborder data flow in their data protection acts, the German data protection law does not contain any special regulation on this subject in the private sector. This situation has not changed with the enactement of the amended Data Protection Act in June 1991. The legislator has still refused to create new provisions on TBDF although many voices in literature have criticised this statutory gap.[22]

Some Hints

However, there are some hints in the new BDSG which may help to solve the problem to TBDF and its legality under German data protection law.

General considerations on TBDF. The German data protection law uses a very restrictive approach with regard to the processing of personal data: In general, all data processing, any data storage and any data transfer has been forbidden in the act. It allows the transfer of personal data merely in two cases: either the data subject has given his written consent to the transfer or the disclosure has expressly been authorised by specific statutory provisions (section 4(1)).[23] If a transfer of data is not based on consent or statute, it is held to be unlawful.

Written consent. This leads to the difficult question of whether TBDF and EDI may be authorised by consent. In fact, it is very rare that data users rely on written permissions of the data subjects. With regard to the amount of data transferred by means of EDI, it is too complicated to ask each data subject for consent. But even if a data user has got the consent, this consent may be void. Some authors [24] have regarded a general consent to any form of data processing to be *contra bonos mores* and invalid.

EDI and statutory authorisation. Therefore, the main question is whether TBDF and EDI may be authorised by statutory provisions. The BDSG contains very detailed and restrictive regulations on data transfer. According to sections 28 and 29, the transfer of data is deemed to be unlawful if the legitimate interests (schutzwurdige Interessen) of the data subject prevail.

But when do the legitimate interests of a data subject prevail in the case of TBDF and EDI? The German literature [25] unanimously distinguishes between two 'constellations' of TBDF: personal data may be transferred to a country that has a data protection law comparable and

equivalent to the German regulations. In this case the data subject has not lost his rights to access, rectification and erasure of data so that the data transfer does not affect his interests. The situation is different, however, if the data are transferred to a country that has no data protection law or imperfect regulations (compared to the German standard). The data subject has a right to be protected against data transfers in favour of 'data havens'. Therefore, the German law allows personal data only to be transferred to states with an 'equivalent' data protection law.

The 'equivalence'. These considerations lead to the main problem of TBDF: what is meant by 'equivalence'?[26] Which states are provided with a data protection law comparable to the German standard? Does the transborder data flow from Germany to Great Britain violate the legitimate interests of data subjects so that it is unlawful?

Up to now, Belgium, Greece, Italy, Spain and Switzerland have no data protection regulations at all.[27] Hence personal data must not be transferred from Germany to these states; such transfer is regarded as unlawful and may even be prosecuted as crime.

Unlike these 'data havens', the British legislator has enacted a detailed Data Protection Act (DPA) which shows many similarities with the German Act: For instance, they both cover automated personal data used in the public and private sectors. The problem of transborder data flow itself has been solved in Great Britain with a special provision (section 39) which is even more detailed than the German regulations. Both acts give data subjects:

- a right of access to records on themselves;
- a right to apply to the court for rectification and erasure;
- a right to claim compensation for inaccuracy of data and loss or unauthorised disclosure.

There are, however, some doubts as to the equivalence of the British Act since there are major differences between these two statutes:

(1) The DPA only protects automated data (section 1(2)) while the German Act also extends to personal data stored in manual records.

(2) The DPA does not contain special provisions regulating the storage and transfer of data; it only applies the Convention of the Council of Europe [28] with regard to some very general and vague data protection principles.

(3) The data protection registrar has never used his power under section 12 to restrict TBDF.[29] Additionally, he is not able to prohibit data traffic to Spain which is merely bound by the European Convention, but has no data protection legislation.[30] This legal gap contrasts to the situation in Germany where a transfer of data to Spain is likely to be regarded as unlawful (see above).

(4) Section 34 of the new German BDSG provides for a right of data subjects to be informed gratuitously which of their personal data are used, for which purpose they are held and to whom they are regularly transferred (in the case of automated data). The British DPA only grants information on the stored data against payment (section 21(1)).[31]

(5) The DPA contains some exemptions which are unknown to German law, such as the provisions on payrolls and accounts (section 32).

Consequently, it has to be decided whether the British Act is equivalent to the German provisions despite these differences. Some authors criticise the British regulations as being too lax.[32] In my opinion, the problem cannot be solved by using sweeping statements. The British DPA has almost the same standard of protection with regard to automated data as has been established in the German Act. Both Acts grant the same protection against the transfer of personal data with the aid of EDI. The fact that the British Act does not include provisions on data stored in manual recordings is irrelevant in EDI cases.

The 'Spanish problem' mentioned above is, in my view, a more difficult issue. If personal data can be transferred to a state without any specific data protection law, the establishment of 'data havens' may be supported by transborder data flow and EDI. A German corporation is, for instance, not allowed to transfer data directly to Spain under German law. The English law may promote the idea of circumventing this regulation by transferring data first to England and then from England to Spain.

It is thus very doubtful whether the English data protection law is equivalent to the German law. A transfer of personal data from the Germany to Britain by EDI may thus be unlawful under the German Data Protection Act.

The Computer Bureaux

The German Act contains another regulation with regard to TBDF focussing on computer bureaux, e.g. persons and corporations who provide services in respect to personal data.

The German Data Protection Act only applies to the transfer of data if the transferee has to be regarded as a 'third person' (Dritter), e.g. a person different from and independent of the transferor (section 2(3)). The Act additionally provides that computer bureaux are in general not third persons in relation to their customers (section 2(9)). Therefore, the disclosure of data to computer bureaux is generally lawful; furthermore, the new German Data Protection Act expressly provides that the customers, but not the computer bureaux, are liable for any violations of the Act (section 11(1)).

If the computer bureau is, however, located abroad, the situation is different: in this case, any disclosure of data is regarded as a transfer of

data to a third person so that the bureau and the customer are responsible for the enforcement of the Act (section 2(9)). This regulation has the effect that transborder data flow to a foreign computer bureau is only lawful under the restrictive conditions mentioned above.

The Proposal for a Council Directive on Data Protection

The actual legal situation may be summarised to the effect that a transfer of personal data from Germany to Great Britain is likely to be unlawful, even in the case of a transfer to a British computer bureaux. Therefore, the different standard of data protection within Europe is likely to become a big problem for TBDF and EDI.

The situation will yet change with the implementation of the future EEC directive on data protection. The Commission has held in the preamble of its proposal for a data protection directive that the directive is necessary to promote an equivalent "level of protection in relation to the processing of (...) date (...) in all the Member States". Thus, EEC directive may be an effective way to create a uniform standard of data protection within Europe so that EDI will be lawful within all EEC member states.

The German authorities have, however, made very strange considerations on the importance of the EEC directive. For instance, the Federal data protection commissioner, Dr Alfred Einwag, has stressed at a conference in Munich on 30 January 1992 that the EEC directive will only establish a minimum regime of data protection. In his opinion, the EEC 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 to this way of thinking. Article 1(2) of the EEC 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 that goes beyond the scope of an EEC directive will become an obstacle to the free flow of data within the Community. Therefore, the German authorities would violate Article 8a of the EEC Treaty and the idea of a European market without frontiers by postulating national regulations on TBDF different from the EEC directive. The efforts of the EEC Commission to establish a uniform level of data protection within Europe will force the German legislator to adopt the EEC regulations and change the German Data Protection Act at least with regard to TBDF.

Contractual Regulations on Data Protection

The difficult legal problems mentioned above lead to the question whether contractual arrangements may grant an equivalent data

protection in TBDF cases. In our case, the parties have made some arrangements on TBDF and data protection in a special contract. Does this contract calm German data protection layers? The question has been the subject of controversial discussion in Germany. Many authors stated that effective contractual obligations with regard to data protection may be sufficient to allow TBDF.[33] The former data protection commissioner of the State Hessen, Spiros Simitis, has vigorously objected to this idea.[34]

The controversy has been caused by different views on the effectivity of contractual rights: Simitis believes that the data subject will never be a beneficiary of a contract which has been closed between the data transferor and the transferee; the parties of this contract are free to change the contract and its data protection provisions at any time. This opinion may be true with regard to the English law, which emphasises the Roman tradition of the "privity of contract".[35] The German law, however, allows contracts to be closed on behalf of a third person (section 328 of the Burgerliches Gesetzbuch). Therefore, Simitis seems to have forgotten that access or erasure rights of a data subject may be embodied in a contractual agreement between data transferor and transferee.

However, the German courts have not yet solved all the problems involved with this special form of contract. There are a lot of questions which remain ambiguous and unclear:

(1) Support the transferee refuses rectification of data to the data subject in breach of the contract. The data subject may then terminate the contract and claim compensation.[36] But what about the transferor? Is he allowed to terminate the contract, too? Precedents with regard to this problem do not exist. Some authors have held that a contract closed in favour of a third person may only be terminated by one party if the third person consents.[37] Other commentators suppose that the parties to a contract may terminate the contract without any consent of the third person.[38]

(2) The parties may reserve the right to change the contractual rights of the third person (cf. section 328(2) of the BGB). This reservation may be included expressly in the contract; it may also be made implicitly.[39] There are some discussions in the literature as to whether this reservation must be recognisable for the third person.[40] Thus, the parties of a contract on EDI may easily cancel the rights of a data subject.

(3) If the data subject asserts his contractual rights, the transferee may refuse to grant access or rectification of a data if the transferor has not fulfilled his contractual obligations towards the transferee (section 334 of the BGB). In the present case, the employees will thus not be able to realise their rights in regard to the British company, if the company has not received all relevant data from Germany. This problem may only

be solved in the case of contrary contractual provisions; it has, however, been discussed controversially if section 334 is mandatory or not.[41]

Consequently, a contract on TBDF has to be drafted to the effect that the data subject has inviolable and unchangeable rights equivalent to his rights under the German Data Protection Act; otherwise, the contract does not have the effect of transborder data flow being lawful.

The legal situation is likely to become more difficult with the future EEC directive on data protection mentioned above. According to Article 24 of the the proposal, the transfer of personal data to non-EEC countries shall only be lawful if these countries ensure "an adequate level of protection". This regulation has been amended by the European Parliament [42] to the effect that the transfer of "particular categories of specified data" (whatever that means) may "be prohibited in order to prevent damage to data subjects interests from an inadequate level of protection".[43]

Furthermore, the first proposal presumes that contractual arrangements on TBDF and data protection are in general invalid if the third country has no adequate level of protection. The proposal exceptionally accepts TBDF contracts under special conditions (Article 25):

- The controller of the file has to give sufficient proof that an adequate level of protection will be provided.
- The Member State in which the file is located has to authorise such a transfer of data.
- The EEC commission and all Member States have to be informed, with a 10-day period in which notice of opposition may be given.

On the one hand, this procedure is too bureaucratic and cumbersome. Supposing that the USA have a minor standard of data protection compared to Europe the transfer of any personal data from Europe to the USA 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, the procedure endangers the protection of privacy. Article 25 includes a lot of ambiguous terms. What is, for instance, the meaning of "adequate level of protection"? Does this term refer to the EEC standard of protection or to the national data protection regulations of an EEC member state? How can a controller of a file guarantee this level of protection? By means of a contract? Which clauses should be included in the contract to ensure an adequate level of protection?

A period of 10 days is too short in the case of modern telecommunications networks and the expanding use of EDI. If a

corporation transfers a huge amount of personal data to non-EEC countries via satellites, the EEC commission and the EEC member states have to check very carefully whether these transfer comply with the European standard of data protection. It is absurd to give them 10 days in order to give a notice of opposition.

If the requirements set up in Articles 24 and 25 are not realised, any transfer of personal data is held to be unlawful even in the case of consent of the person concerned. This is too rigid: why should a person be protected against a transfer of his data if he does not want to be protected? The European Convention on Human Rights and most national constitutions stress the individual right of self-determination. In my view, this right is violated if a person concerned is not allowed to consent to transborder data flows. Fortunately, this problem has recently been regarded by the European Parliament which amended section 24 to the effect that TBDF will always be lawful under express consent of the data subject.[44]

Conclusion

The existing legal framework has put heavy restrictions on the use of EDI for the purpose of transborder data flows. The example of a transfer of personal data from Germany to Britain has demonstrated that difficult problems of private international law and various aspects of data protection may prevent transborder data flows.

These problems have their own origin in the fact that the conflict of laws and data protection have almost been regarded as national issues. European regulations on these subjects are still missing. With regard to private international law, uniform European rules have only been established with regard to the contract law (see above). The European states have not been able to develop equivalent national regulations on data protection. A European standard of data protection cannot be created with the aid of the data protection principles embodied in the Convention of the Council of Europe, because these principles are too vague and empty.

The importance of these problems will increase with the development of the Common European Market in 1993. The EEC Commission certainly has tried to deal with the TBDF issue and published their long-awaited proposal for a directive on data protection. These efforts have, however, been subject to worldwide criticism [45] especially because the EEC proposal has been prepared in detrimental haste and under the pressure of professional lobbyists. The German authorities [46] have already rejected the proposal; they think that the proposal might abrogate the constitutional principles of data protection, as:

- the idea of the German Constitutional Court [47] that all personal data should be protected in the same way so that special categories of sensitive data do not exist (cf. Article 17 of the EEC proposal);
- the idea of the German Constitutional Court that any controller of a file either computer file or non-computer file) shall respect the privacy of a data subject, even the controller is working for a non-profit making body (cf. Article 3(2)(b) of the proposal), a credit-information organisation or the press (Article 19);
- the idea of German Constitutional court that the regulations on the processing and transfer of data should be made using clear and unambiguous terms as far as possible (cf. the term "national security" in Article 15(1)(a) of the proposal).

Consequently, there will be a lot of discussion in the future concerning the EEC directive on data protection and its implementation into German law.

Correspondence

Dr Thomas Hoeren, Institut für Kirchenrecht, Universitatsstr. 14-16, D-4400 Munster, Germany.

Notes

[1] This article is based upon a paper presented at the Third National Conference on Law, Computers and Artificial Intelligence which took place in Aberystwyth (Wales) from 30 March to 1 April 1992.

[2] Cf. Briat (1988) Personal Data and the Free Flow of Information, in Hansen et al (Eds) *Freedom of Data Flows and EEC Law*, p. 47. Deventer.

[3] Cf. Millard (1988) Transborder data flows: the European perspective, paper presented at the CLA conference on Distribution, Access and Communication, Amsterdam, 1-3 June.

[4] See Bing (1991) Reflections on a data protection policy for 1992, *YLCT*, 5, p. 175.

[5] Kirby (1980) Data flows and the basic rules of data privacy, *Stanford Journal of International Law*, 16, pp. 27-66, at p. 29.

[6] See the profound doctoral thesis of Ellger (1990) *Der Datenschutz im grenzuberschreitenden Datenverkehr. Eine rechtsvergleichende und kollisionsrechtliche Untersuchung*, Baden-Baden: Nomos, p. 584 et seq.

[7] Rigaux (1980) La loi applicable a la protection des indivudues a l'egard du traitement de donnees a caractere personnel, *Revue critique de Droit International Prive*, p. 443 et seq.; cf. Koch (1991) Rechtsvereinheitlichung und Kollisionsrecht, *Recht der Datenverarbeitung*, pp. 110-111.

[8] Bergmann (1985) *Grenzuberschreitender Datenschutz*, Baden-Baden (Nomos), p. 239 et seq.; Fraysinnet/Kayser (1979). La loi du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertes et le decret du 17 juillet 1978, in

other doctrines see *Munchener Kommentar zum BGB*/Martiny, 2nd edn, Munich: Beck, 1991, Article 34 EGBGB, Note 25 et seq. with further references.

[20] For the text of the Convention see North (Ed.) (1982) *Contract Conflicts*, London and Morris & North (1984) *Cases and Materials on Private International Law*, London: Butterworths, pp. 459-465.

[21] Cf. Bundesrats-Drucksache 222/1/83, p. 9; see Martiny (1987) Der deutsche Vorbehalt gegen Art. 7 Abs. 1 des EG-Schuldvertragsubereinkommens vom 18.6.1989 – Seine Folgen fur die Anwendungen auslandischen zwingenden Rechtes, *Praxis des Internationalen Privat – und Verfahrensrechts*, p. 277 et seq.

[22] See Simitis & Dammann (1981) *Commentary on the Bundesdatenschutzgesetz*, 3rd edn, Baden-Baden: Nomos, s. 22, Note 51; Simitis (1978) Grenzuberschreitender Datenaustausch – Notwendige Vorbemerkungen zu einer dringend erforderlichen Regelung, *Festschrift fur Murad Ferid zum 70. Geburtstag*, Munich: Beck, pp. 354-375.

[23] This iron rule has been called the "Magna Charta of the German data protection law".

[24] Auernhammer (1981) *BDSG*, 2nd edn, Munich: Beck, Sect. 4, Note 34; cf. Ellger, op. cit., p. 412.

[25] Simitis & Dammann, op. cit., s. 22, Rdn. 54; Ordemann & Schomerus (1988) *BDSG*, 4th edn, Munich: Beck, s. 24, Anm. 5; Auernhammer, op. cit., s. 24, Rdn. 9.

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

[27] See the table prepared by Christopher Millard in Chalton & Gaskill (1991) *Encyclopedia of Data Protection*, London: Sweet & Maxwell, No. 7-630.

[28] Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981; the text of the convention may be found in Chalton & Gaskill (191) *Encyclopedia of Data Protection*, London: Sweet & Maxwell, No. 7-195. Cf. Evans (1981) European data protection law, *American Journal of Comparative Law*, 29, p. 571 et seq.

[29] Napier (1990) Vertragliche Losungen im grenzuberschreitenden Datenverkehr, *Recht der Datenverarbeitung*, p. 214.

[30] Cf. Aldhouse (1991) UK data protection – where are we in 1991? *YLCT*, 5, p. 187 with reference to other problems of this section of the DPA.

[31] Cf. Walden & Edwards, (1990) Data protection, in Reed (Ed.) *Computer Law*, London, pp. 216-217.

[32] National Council for Civil Liberties 1984, para. 2.1; cf. Ellger, op. cit., p. 388; Savage & Edwards (1986) Transborder data flows: the European convention and the United Kingdom legislation, *International & Comparative Law Quarterly*, 35, p. 710.

[33] Ordemann & Schomerus, op. cit., 24, Note 5; Gallwas, Schweinoch & Schwappach (1978) *Bundesdatenschutzgesetz*, Stuttgart: Kollhammer, 24,

Note 84; Schwappach (1978) Internationale Datenflusse im Bereich der Industrie, *Datenschutz und Datensicherung*, p. 24; ibid. (1980) Grenzuberschreitender Datenverkehr und Datenschutz, *Wirtschaft und Verwaltung*, p. 32 et seq. Even the Data Protection Commissioner of Hamburg has supported his concept; see the Eighth Report of the Commissioner, November 1989, p. 130f.; Tenth Report of the Commissioner, November 1991, p. 162.

[34] Simitis & Dammann, op. cit., s. 22, Note 55.

[35] *Dunlop v. Selfridge*, AC 847 (1915); *Jackson v. Horizon Holidays Ltd*, 1 *WLR* 1468 (1975); cf. Napier (1990) Vertragliche Losungen fur das Problem des gleichwertigen Datenschutzes im grenzuberschreitenden Datenverkehr, *Recht der Datenverarbeitung*, p. 215; Ehmann (1991) 'Vertragslosungen' auf der Basis der EG-Datenschutzrichtlinie, *Computer und Recht*, p. 234.

[36] Oberlandesgericht Munich, *Rechtspfleger*, 1972, p. 32; Landgericht Bonn, *Neue Juristische Wochenschrift*, 1970, 1084.

[37] Soerge & Hadding (1990) *Burgerliches Gesetzbuch*, 12th edn. Stuttgart: Kollhammer, s. 328, Note 45; Dorner (1985) *Dynamische Relativitat*, Munich: Beck, p. 304 et seq.

[38] Grottwald (1985) *Munchener Kommentar zum Burgerlichen Gesetzbuch*, 2nd edn, Munich: Beck, s. 335, Note 6; Erman & Westermann (1990) *Kommentar zum Burgerlichen Gesetzbuch*, 8th edn, Munster: Aschendorff, s. 335, Note 2.

[39] Bayerisches Oberstes Landgericht, *Mitteilungen der Rheinischen Notarkammer*, 1989, p. 111.

[40] Cf. Staudinger & Kaduk (1979) *Kommentar zum Burgerlichen Gesetzbuch*, 12th edn, Berlin: de Gruyter, s. 328, Note 117; *Reichsgerichtsratekommentar zum BGB*/Ballhaus, 10th edn, Stuttgart: Kollhammer, 1967, s. 328, Note 38 with further references.

[41] Cf. Landgericht Frankfurt, Judgement of 1 September 1982 (2/22-155/82), *Neue Juristische Wochenschrift*, 1983, p. 53; Bundesgerichtshof, Judgement of 17 January 1985 (VII ZR 63/84), *BGHZ*, 93, p. 275 (*Neue Juristische Wochenschrift, 1985, p. 1458*) against Gernhuber (1989) *Das Schuldverhaltnis*, Munich: Beck, s. 20, IV 3c.

[42] Amendments adopted by the European Parliament on 11 May 1992, reprinted in J. Dumotier (Ed.) (1982) *Recent Developments in Data Privacy Law*, Leuven: Leuven University Press, p. 159ff.

[43] E.P. No. 78 This amendment demonstrates that the European Parliament has a more liberal view with regard to transborder data flow to non-EEC states. The way in which the parliament has drafted its amendment indicates that TBDF shall be held to be lawful in general. It may only be prohibited if a member state can prove an inadequate and dangerous level of protection in the third country.

[44] 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".

[45] See, for instance, Knauth (1990) Datenschutz und grenzuberschreitender Datenverkehr in der Kreditwirtschaft, *Wertpapier-Mitteilungen*, p. 213; Ellger

Datenschutz und europaischer Binnenmarkt, *Recht der Datenverarbeitung*, (1991) pp. 134-135.

[46] Cf. Walz (1992) Europaische Gemeinschaft – Informationeller Grossraum und Harmonisierung des Datenschutzes, paper presented at the IIR conference Datenschutz in der Industrie, Munich, 30 January.

[47] Federal Constitutional Court, Judgement of 15 December 1983, BVerfGE 65, 1 (*Neue Juristische Wochenschrift*, 1984, p. 419); Judgement of 9 March 1988, *Neue Juristische Wochenschrift*, 1988, p. 2031; cf. Federal Supreme Court, Judgement of 15 December 1983, *Neue Juristische Wochenschrift*, 1984, p. 1889; Federal Labour Court, Judgement of 6 June 1984, *Neue Juristische Wochenschrift*, 1984, p. 2910.