The Transfer of Data Abroad by Private Sector Companies: Data Protection Under the German Federal Data Protection Act

By Jutta Geiger[*]

A. Introduction

Private sector companies face a major challenge in ensuring compliance with the many detailed data protection rules that can apply. The compliance burden is further increased if a business enterprise operates in several countries with different data protection rules. This may complicate the exchange of data within the enterprise. The purpose of this article is to plot a path through these rules governing the transfer of personal data abroad.

German law distinguishes between the general provisions on the protection of personal data for private sector companies under the *Bundesdatenschutzgesetz* (BDSG – German Federal Data Protection Act)[1] and the specific data protection provisions specified in numerous enactments and regulatory provisions (e.g., *Teledienstedatenschutzgesetz* [Teleservices Data Protection Act] , the *Telekommunikationsgesetz* [Telecommunications Act] , and the *Mediendienste-Staatsvertrag* [Interstate Agreement on Media Services]). Where specific data protection provisions apply, they take precedence over the provisions of the BDSG.[2]

The BDSG only applies to information concerning the personal or material circumstances of an identified or identifiable individual (personal data); it does not cover information relating to legal entities.[3] The BDSG applies to private sector companies to the extent that they process or use personal data by means of data processing systems or collect data for such systems. It also applies to private sector companies in so far as they process or use personal

[*]Dr Jutta Geiger is a *Rechtsanwältin* (German lawyer) and a *Fachanwältin für Verwaltungsrecht* (specialist lawyer for Administrative Law) working in the Frankfurt office of Ashurst Morris Crisp, e-mail: jutta.geiger@ashursts.com. The author thanks her colleague Richard Best for valuable comments on the draft of this article.

[1] Bundesdatenschutzgesetz of 20 December 1990, last amended by an act of 21 August 2002. The amended version was published on 14 January 2003, Federal Law Gazette (*Bundesgesetzblatt*) vol. I 2003, p. 68. An English translation of the Act as of 1 January 2002 is available on the internet: www.bfd.bund.de/information/bdsg_eng.pdf.

[2] Section 1 (3) of the BDSG.

[3] Section 3 (1) of the BDSG.

https://doi.org/10.1017/S2071832200016394 Published online by Cambridge University Press

data in or from non-automated filing systems or collect data for such systems.[4] A non-automated filing system is any non-automated collection of personal data which is similarly structured and which can be accessed and evaluated according to specific characteristics.[5]

The requirements as to the collection, processing and use of personal data by private sector companies are provided for in sections 27-31 of the BDSG. In addition, compliance is required in respect of the general provisions in sections 1-11 of the BDSG.

B. Obligatory Registration and the Data Protection Official

As a rule, private sector companies have to notify the competent supervisory authority prior to putting automated personal data processing procedures into operation.[6] There are two exceptions to this rule. First, registration is not required if the controller has appointed a data protection official (this is obligatory if more than four employees are concerned with the collection, processing or use of personal data).[7] Secondly, provided that no more than four employees are concerned with the collection, processing or use of the data, registration is also not required if the controller processes or uses personal data for its own purposes and either consent has been obtained from the data subject or the collection, processing or use serves the purpose of a contract or a quasi-contractual fiduciary relationship with the data subject.[8]

Neither exception applies, however, if companies store personal data in the course of business for the purpose of transfer, irrespective of whether the data is transferred in anonymised form (e.g., credit inquiry agencies, or market and opinion research institutes).[9] In those cases they have to register automated processing procedures irrespective of the number of employees concerned with data processing and irrespective of the appointment of a data protection official.

The details to be provided in the obligatory registration are evident from the registration form. Registration forms are available from the competent supervisory authorities. All private sector companies are supervised by authorities of the *Länder* (Federal States)[10] – for example in Hesse, these are the *Regierungspräsidien* (Regional Councils) – with the exception of postal and telecommunications companies which are supervised by the *Bundesbeauf-*

[4] Section 1 (2) no. 3 of the BDSG.

[5] Section 3 (2) sentence 2 of the BDSG.

[6] Section 4d (1) of the BDSG.

[7] Section 4d (2) of the BDSG.

[8] Section 4d (3) of the BDSG.

[9] Section 4d (4) of the BDSG.

[10] Section 4d (1) in connection with section 38 (6) of the BDSG.

tragter für den Datenschutz (Federal Commissioner for Data Protection).[11] Registration cannot be effected online.

As mentioned above, private sector companies where more than four employees are occupied with the collection, processing or use of personal data are required to appoint a data protection official within one month of commencing their activities. If data is not collected, processed or used automatically, there is no such obligation if less than 20 persons are permanently employed for this purpose.[12] A data protection official is to be appointed irrespective of the number of employees if special types of personal data, as defined in section 3 (9) of the BDSG (e.g., information on a person's racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life) or personal data that is intended to appraise the data subject's personality are automatically processed.[13] The same applies if personal data is collected, processed or used in the course of business for the purpose of transfer or for the purpose of transfer in anonymised form.[14] The appointment of the data protection official must be made in writing.[15]

The data protection official shall – if necessary, upon consultation with the competent supervisory authority – do his or her utmost to comply with the provisions pertaining to data protection.[16] To that end, he/she must monitor the proper use of the data processing programs and familiarize the persons dealing with data processing with the relevant provisions.[17] In addition, he/she is responsible for providing information on stored data and to address complaints in connection with the collection, storage and use of personal data.[18] Finally, in the event of supervisory measures, the data protection official is the contact person for the competent supervisory authority.[19]

The data protection official shall be directly subordinate to the head of the private sector company. He or she shall not, however, be bound by instructions given by management in his/her limited tasks of monitoring and rendering advice.[20]

---

[11] Section 4d (1) of the BDSG.

[12] Section 4f (1) sentence 3 of the BDSG.

[13] Section 4f (1) sentence 6 in connection with section 4d (5) of the BDSG.

[14] Section 4f (1) sentence 6 of the BDSG.

[15] Section 4f (1) sentence 1 of the BDSG.

[16] Section 4g (1) sentences 1 and 2 of the BDSG.

[17] Section 4g (1) sentence 3 of the BDSG.

[18] Section 4g (2) sentence 2 and section 4f (5) sentence 2 of the BDSG.

[19] This may be inferred from section 38 (5) sentence 3 of the BDSG.

[20] Section 4f (3) of the BDSG.

The data protection official must possess the requisite expertise and reliability to perform his or her duties. This requires that the data protection official is familiar with data processing processes within the business enterprise and has basic knowledge of the relevant data protection law. Requisite reliability is always lacking if the data protection official is at the same time entrusted with tasks which may result in a conflict of interests. For this reason, the head of the personnel department or the head of the EDP (electronic data processing) may not be appointed as data protection official.[21] The data protection official need not be employed in the business enterprise, i.e., external data protection officials may also be appointed.

C. Permissibility of Data Processing

Pursuant to section 4 of the BDSG, the collection, processing and use of personal data is permissible only if the Act or another legal provision so allows or stipulates or the data subject has consented to it. Personal data is generally to be collected from the data subject who is to be informed about the identity of the controller and the purpose of the collection, processing and use of personal data.

For private bodies, the statutory permission to collect, process and use personal data is found in sections 28-30 of the BDSG and – as regards the transfer of data abroad – sections 4b and 4c of the BDSG.

The requirements as to effective consent are provided for in section 4a of the BDSG. Consent shall be effective only when based on the data subject's free decision. This requires that the data subject was informed in advance of all relevant circumstances for the purpose of making his or her decision.[22] Furthermore, consent must be given without the data subject being put under duress. In this regard, a relevant consideration is whether the data subject was, due to a certain situation (e.g., in an employment relationship) under social or economic duress to give its consent.[23]

As a rule, consent must be given in writing to be effective, i.e., it requires the hand-written signature or a qualified electronic signature in accordance with the German *Signaturgesetz* (Digital Signature Act).[24] Opinion is divided as to the circumstances in which, in exceptional cases, those requirements may be waived.[25] Special urgency justifies a waiver of the written form requirement.[26] As an alternative to the written form requirement or an elec-

[21] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4f, note 26.

[22] Section 4a (1) sentence 2 of the BDSG.

[23] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, notes 6-9.

[24] Federal Law Gazette vol. I 2001, p. 876.

[25] Restrictive: Simitis, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 4a, notes 35-37 and 45-53. Less restrictive: Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, note 13.

[26] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, note 13.

tronic signature, only express oral consent can be considered.[27] For instance, in opinion polls conducted over the telephone, consent given over the telephone is deemed to be sufficient if written consent is unable to be obtained or if the interviewer's work would be rendered unreasonably more difficult.[28] Consent given implicitly is insufficient and consent may not be replaced by the granting of a right of revocation.[29]

D. Transfer of Data Abroad

With the revision of the BDSG by an amending Act dated 18 May 2001, German law for the first time prescribed the circumstances in which private bodies are permitted to transfer personal data abroad. In doing so it implemented the provisions of the Data Protection Directive of the European Community.[30]

In relation to the provisions governing the admissibility of data transfer abroad, a distinction is made between those countries in which the EC Data Protection Directive is applicable – in addition to the Member States of the European Union (EU), they include the Member States who are signatories to the Treaty on the European Economic Area (EEA), i.e., Liechtenstein, Norway and Iceland – and other countries (third countries). Transfers within countries in which the EC Data Protection Directive applies are deemed to be "within the country", i.e., the cross-border transfer of data is subject to the same conditions as the transfer of data between bodies domestically (general transfer conditions).[31] On the other hand, additional conditions must be complied with in respect of transfer of data to third countries unless those third countries provide for a comparable level of data protection.[32]

I. Definition of Data Transfer

The concept of transfer is defined in section 3 (4) no. 3 of the BDSG. It means the disclosure to a third party of personal data stored or obtained by means of data processing either through transmission of the data to a third party or through the third party inspecting or retrieving data held ready for inspection or retrieval. The decisive factor in the case of data transfer is not whether the recipient stores the data.[33]

Pursuant to section 3 (8) of the BDSG, a “third party” is any natural person or legal entity other than the controller with the exception of the data subject and the persons and bodies

[27] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, note 13.

[28] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, note 13.

[29] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4a, notes 14 and 20.

[30] Directive 95/46/EC, Official Journal L 281 p. 31.

[31] Section 4b (1) of the BDSG.

[32] Section 4b (2) of the BDSG.

[33] Schaffland/Wiltfang, BDSG, Kommentar, last update: March 2003, section 3, note 57.

commissioned to collect, process or use personal data in Germany, in another Member State of the European Union or in another state party to the Agreement on the European Economic Area.

By use of the wording "other than the controller", the law focuses on the legal rather than the economic entity. Accordingly, data exchange between separate legal entities which are economically affiliated (groups of companies), or the disclosure of personal data by a legally independent body of a business enterprise to another legally independent body of the same business enterprise, constitutes a transfer.[34] A parent company is thus a third party in relation to its subsidiary.

On the other hand, there is no transfer if the data is disclosed within the same legal entity (e.g., from one department or branch to another). If the branch is, however, situated in a third country and governed by that law, it may, in the opinion of some commentators, be deemed to be a third party because otherwise personal data could be transmitted from the European Community, in which there is uniform data protection, without any inspection being conducted .[35]

Commissioned collection, processing and use of personal data is governed by section 11 of the BDSG. Where data is commissioned to be processed, responsibility for compliance with the relevant statutory provisions rests with the principal. The agent, who may process the data only as instructed by the principal, is treated as part of the principal and not as a separate entity. As agents situated in third countries are deemed to be third parties, the disclosure of personal data to them is governed not by section 11 of the BDSG, but by the provisions on data transfer to third countries.

II. General Transfer Conditions

If personal data is collected from the data subject for the purpose of transfer, the controller is obliged pursuant to section 4 of the BDSG to inform him or her of the categories of recipients in so far as the circumstances of the individual case provide no grounds for the data subject to assume that data will be transferred to such recipients. The admissibility of the transfer of personal data is subject to the general requirements of sections 28-30 of the BDSG.

Section 28 (1) of the BDSG regulates the collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes. Section 28 (2) and (3) of the BDSG regulate the permissibility of transfer of personal data for another purpose (among others, for purposes of advertising, market and opinion research, where the data is compiled in lists or is otherwise combined concerning members of a group of persons). Pursuant to section 28 (4) of the BDSG, data transfer for the purposes of advertising

[34] Dammann, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 3, note 239.

[35] Schola/Gomerus, BDSG, Kommentar, 7th edition 2002, section 3, note 53.

or market and opinion research is prohibited if the data subjects object. Section 28 (5) of the BDSG concerns the proposition that a recipient of personal data can only use it for the purpose for which it was transferred. Section 28 (6)-(9) of the BDSG prescribe the conditions under which the collection, processing and use of special types of personal data (sensitive data) is permitted. Section 29 of the BDSG concerns the collection and storage of data in the course of business for the purpose of transfer and section 30 of the BDSG concerns the collection and storage of data in the course of business for the purpose of transfer in anonymised form. Section 31 BDSG states that personal data stored for data protection control, security or the operation of processing systems is only to be used for such purposes.

Section 28 (1) of the BDSG, which relates to the processing of data as a means of fulfilling the controller's own business purposes, is the most relevant of these three provisions because it applies to the transfer of personal data of employees or customers. The following discussion is therefore limited to this provision.

Section 28 (1) of the BDSG specifies three situations in which the transfer of personal data is permitted.

First, in the event that a contractual relationship or a quasi-contractual fiduciary relationship exists between the controller processing the data and the data subject, transfer of data is permitted provided it serves the purpose of that relationship. In this regard, a contract may specifically contemplate the disclosure of data to third parties such that there would be no difficulty in establishing this requisite purpose (e.g., a travel agent selling flights will have to disclose personal data of customers to the air lines to book the flights). Similarly, the purpose of a quasi-contractual fiduciary relationship (for instance, prior to entering into an agreement), may contemplate the disclosure of data, e.g., in relation to obtaining information on the credit worthiness of the customer.

Secondly, the transfer or use of personal data for another purpose is permitted to the extent that it is necessary to safeguard the legitimate interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from transfer. A data controller is therefore required to consider whether its own interests in transfer are overridden by the data subject's interests in the data not being transferred, bearing in mind that the interests of each must be "legitimate", which entails a reasonable assessment of the circumstances giving rise to the interests and the effect which a transfer could have on both sides' interests. In this context, one may note that the transfer of personal data within the framework of a due diligence during a corporate acquisition may be permitted.[36] However, the transfer of such data may equally be prohibited if the information requirements of the potential purchasers can be met by a transfer of data in anonymised form.

Thirdly, data may be transferred if the data is generally accessible or if the controller would be entitled to publish it, unless the data subject's legitimate interest in his data being ex-

[36] Cf. Simitis, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 28, note 89.

cluded from transfer clearly outweighs the justified interest of the controller of the filing system.

Section 28 (1) of the BDSG states further that in connection with the collection of personal data, the purposes for which the data is to be processed or used are to be specified in concrete terms. Although that specification need not necessarily be made in writing to be effective, a written specification is advisable to avoid any doubt. Because the legislation requires a concrete and thus unambiguous specification of purposes, the controller of the filing system is to be held responsible in cases of doubt, i. e., in cases of doubt, a change of purpose is to be assumed. If a data controller does change or broaden the purpose of transfer, it can and ought to check whether the transfer is permissible under section 28 (2) and (3) of the BDSG.

III. Legal Requirements for the Transfer of Data to Third Countries

The transfer of personal data to third countries is permitted only if, in addition to the general transfer conditions, (section 4 and sections 28-30 BDSG), the additional requirements of sections 4b, 4c of the BDSG are satisfied.

Pursuant to section 4b (2) sentence 2, the transfer of data to a third country is permissible only if there is an adequate level of data protection there. If that is not the case, one needs to consider whether the exceptions in section 4c (1) of the BDSG apply. If those exceptions do not apply, the competent supervisory authority may authorise individual transfers of data or certain types of transfers of personal data to bodies in third countries as per section 4c (2) of the BDSG if the controller provides evidence of adequate safeguards with respect to the protection of privacy and the exercise of corresponding rights, such safeguards resulting from contractual clauses or binding corporate regulations.

IV. Adequate Level of Data Protection

Pursuant to section 4b (2) sentence 2, the transfer of data to a third country ought not be effected if the data subject has a legitimate interest in excluding the transfer, in particular if an adequate level of data protection is not guaranteed. Section 4b (3) of the BDSG contains a non-exhaustive list of the circumstances to be taken into account when considering the adequacy of the recipient's data protection. Particular consideration shall be given to the nature of the data, the purpose, the duration of the proposed processing operation, as well as the country of origin, the recipient country and the legal norms, professional rules and security measures which apply to it.

Pursuant to section 25 (4) of the Data Protection Directive of the European Community, the European Commission may determine that a third country does not guarantee an adequate level of data protection. Pursuant to section 25 (6) of the Directive, the European Commission may determine that a third country guarantees an adequate level of data protection on the basis of its national legal provisions or international obligations. Those determinations are binding on EU Member States. To date, the Commission has only issued a general posi-

tive determination in favour of Switzerland[37] and Hungary.[38] It has also made a positive determination for Canada for those recipients subject to the Canadian "Personal Information Protection and Electronic Documents Act" of 13 April 2000.[39]

In addition, the Commission issued a decision stating that there is a sufficient level of data protection in relation to personal data which is transferred from a Member State to the United States of America if principles of "safe harbor" in relation to data protection attached to the decision as schedule I are complied with.[40] Those principles implement the "Frequently Asked Questions" (FAQ), attached to the decision as schedule II, contained in guidelines issued by the U.S. Department of Trade & Commerce on 21 July 2001. The U.S. Department of Trade & Commerce or a body nominated by it keeps a list of the organisations which are obligated to adhere to the Safe Harbor Principles. This can be accessed by the public on the Internet.[41]
Finally, the Commission determined that the standard contractual clauses, attached as a schedule to its decision of 15 June 2001,[42] ensure adequate guarantees for the transfer of personal data from Member States of the EU to third countries. The decision obliges Member States to recognise that business undertakings or organisations which use such standard clauses in agreements on the transfer of personal data to third countries, guarantee an adequate level of data protection. Another decision of 27 December 2001 contains standard contractual clauses for the transfer of personal data by data controllers in the EU to a recipient merely functioning as an agent in a third country. [43]

V. Data Transfer to Third Countries Without an Adequate Level of Data Protection

Section 4c (1) sentence 1 of the BDSG prescribes the conditions, or exceptions, under which a transfer of data to bodies in third countries is, in exceptional cases, also permitted notwithstanding that an adequate level of data protection cannot be guaranteed.

First, the provision states that the transfer is permitted if the consent of the data subject has been obtained. As the Act already contains the general rule that consent is sufficient to allow the transfer of personal data[44] this provision simply clarifies that that general rule also applies to the transfer of data to third countries without an adequate level of data protection. In such a case, consent is only effective if the data subject has not only been informed about

[37] Decision of 26 July 2000 (2000/518/EC), Official Journal L 215 of 25 August 2000, p. 1.

[38] Decision of 26 July 2000 (2000/519/EC), Official Journal L 215 of 25 August 2000, p. 4.

[39] Decision of 20 December 2001 (2001/02/EC), Official Journal L 2 of 4 January 2002, p. 13.

[40] Decision of 26 July 2000 (2000/520/EC), Official Journal L 215 of 25 August 2000, p. 7.

[41] www.export.gov/safeharbor.

[42] Decision 2001/497/EC, Official Journal L 181 of 4 July 2001, p. 19.

[43] Decision 2002/16/EC, Official Journal L 6 of 10 January 2002, p. 52.

[44] Section 4 (1) BDSG.

the scope and purpose of the transfer of data, but also about the potential inadequacy of data protection on the part of the body receiving the data.[45]

Second, the transfer of data to third countries is permitted if it is necessary for the conclusion or performance of a contract between the data controller and the data subject. This condition may be fulfilled, for example, if an employment contract includes a clause according to which the employee has to perform a part of his or her duties with an affiliated company in a third country.[46] However, if it is not evident from the employment contract that the contract also relates to the affiliated company, a transfer of personal data to this company is only permissible with the consent of the employee.[47]

The transfer of data is also permissible if the transfer is necessary for the conclusion or performance of a contract which has been or is to be entered into in the interest of the data subject between the controller and a third party. If, for example, a data subject concludes an agreement for a trip to a third country, the travel agent needs to arrange for accommodation in the third country and may transfer the requisite data of the data subject there for that purpose. Should the data in the third country also be given to a tour operator on site for the promotion of tour offers, the transfer of data is not necessary to perform the agreement and thus requires the consent of the data subject. [48]

Furthermore, data may also be transferred if the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims or if the transfer is necessary to protect the vital interests of the data subject. Important public interests are unlikely to exist in the private sector. Vital interests may be deemed to exist if medical data is required to be transferred and the data subject is unable to give his or her consent.[49] Finally, it is permissible to transfer data from public registers, such as from the Commercial Register in a third country with an inadequate level of data protection.

The recipient body is to be informed that the transferred data may be processed or used only for the purpose for which it has been transferred.[50]

VI. Official Authorization

[45] Cf. Däubler, Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 4th edition 2002, note 167.

[46] Cf. Simitis, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 4c, note 13-14.

[47] Cf. Simitis, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 4c, note 15.

[48] Cf. Simitis, in: Simitis (editor), Kommentar zum Bundesdatenschutzgesetz, 5th edition 2003, section 4c, note 12.

[49] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4c, note 5.

[50] Section 4c (1) sentence 2 of the BDSG.

If none of the exceptions in section 4c (1) of the BDSG applies, the competent supervisory authorities may approve individual transfers or certain categories of transfers of personal data pursuant to section 4c (2) of the BDSG if the controller provides evidence of adequate safeguards with respect to the protection of privacy and exercise of corresponding rights. For the transfer of data within globally active groups, it is advisable to establish an internal level of data protection by way of "Codes of Conduct" which apply across the group.[51]

E. Summary

A transfer of data exists if the stored data or personal data obtained by data processing is disclosed to a natural person or legal entity other than the controller or is stored for inspection or retrieval. The internal disclosure of data within the business enterprise to another department or branch does not constitute a transfer of data whereas the disclosure of data to an affiliated business undertaking – unless such affiliated business undertaking is commissioned to process the data – does constitute a transfer of data.

In the case of the transfer of data abroad, a distinction must be made between countries in which the Data Protection Directive of the European Community is applicable (Member States of the EU, Liechtenstein, Norway and Iceland) and other countries (third countries). The transfer of data to third countries is subject to special requirements.

In the case of a transfer of data to third countries, in addition to the general transfer conditions in sections 4, 28-30 of the BDSG having to be fulfilled, the requirements of section 4b of the BDSG (adequate level of data protection), a fact constituting an exception as provided for under section 4c (1) of the BDSG or an official authorisation pursuant to section 4c (2) of the BDSG must also be fulfilled.

However, to the extent that specific conditions for transfer cannot be met, personal data may be transferred if the data subjects' free consent, either in writing or by way of qualifying electronic signature, can be obtained.

[51] Gola/Schomerus, BDSG, Kommentar, 7th edition 2002, section 4c, note 9.