GERMANY

Law on Protection against the Misuse of Personal Data in Data Processing (Federal Data Protection Law - BDSG) of the 27th January 1977

Contents

Part I General provisions
1. Purpose and subject of data protection
2. Definitions
3. Admissibility of data processing
4. Rights of the person concerned
5. Confidentiality
6. Technical and organizational measures

Part II Data processing by public authorities and other public establishments
7. Field of application
8. Processing of personal data on behalf of third parties
9. Storage and modification of data
10. Communication of data within the public sector
11. Communication of data to establishments outside the public sector
12. Public notices concerning stored data
13. Provision of information to the person concerned
14. Correction, blocking and erasure of data
15. Implementation of data protection in the Federal Administration
16. General administrative provisions
17. Appointment of a federal commissary for data protection
18. Legal status of the federal commissary for data protection
19. Duties of the federal commissary for data protection
20. Complaints lodged by the federal commissary for data protection
21. Appeals to the federal commissary for data protection

Part III Data processing by private establishments for their own purposes
22. Field of application
23. Storage of data
24. Communication of data
25. Modification of data
26. Provision of information to the person concerned
27. Correction, blocking erasure of data
28. Appointment of a commissary for data protection
29. Duties of the commissary for data protection
30. Supervisory authority

Part IV Commercial data processing by private establishments for others
31. Field of application
32. Storage and communication of data

1 With minor typographical changes, this text here comes from an English translation of the law made available by the European Commission Directorate General for Industrial and Technological Affairs’ Group of Experts on Data Processing and Privacy, Brussels (Az: III/1125/76-E) as modified by Ursula Gliss.
2 See also Annex at end of the translation.
PART 1 GENERAL PROVISIONS

Section 1 Purpose and subject of data protection

(1) The purpose of data protection is to ensure against the misuse of personal data during storage, communication, modification and erasure (data processing) and thereby to prevent harm to any personal interests that warrant protection.

(2) This Law shall protect personal data which

1. by public authorities or other public establishments (Section 7),
2. by physical or legal persons, companies or other private-law associations for their own purposes (Section 22),
3. by physical or legal persons, companies or other private-law associations for third parties (Section 31) commercially

are stored, modified or erased in data files or are communicated to third parties from data files. Of the provisions of this Law only Section 6 shall apply to personal data which are not intended for communication to third parties and are processed by non-automatic methods.

(3) This Law shall not protect personal data which are processed by undertakings or auxiliary undertakings in the press, radio and film sectors, exclusively for their own journalistic purposes. Section 6(1) shall not be affected by this provision.

Section 2 Definitions

(1) For the purpose of this Law „personal data“ shall mean details on the personal or material circumstances of an identified or identifiable physical person (the person concerned).

(2) For the purposes of this Law

1. storage shall mean the acquisition, recording or retention of data on a storage medium so that they may be further used;
2. communication shall mean the passing of stored data or data acquired directly by means of data processing to third parties in such a way that the data are communicated by the storage unit or are held ready for inspection, i. e., for retrieval;
3. modification shall mean the alteration of the contents of stored data;
4. erasure shall mean the obliteration of stored data, irrespective of the methods used.

(3) For the purposes of this Law
1. a storage unit shall mean any of the persons or establishments specified in Section 1 (2), subparagraphs 1 to 3, which stores data on its own account or has data stored by others;
2. third party shall mean any person or establishment outside the storage unit, with the exception of the person concerned and those persons and establishments which act within the scope of this Law on behalf of third parties as described in subparagraph 1 above;
3. a data file shall mean a collection of data which is assembled on a uniform basis and can be recorded and arranged according to other specific features, irrespective of the methods used. This shall not include document files and collections of document files unless they can be rearranged and evaluated by automatic means.

Section 3 Admissibility of data processing
The processing of the personal data protected by this 'Law shall be admissible in any of the phases mentioned in Section 1 (1) only if
1. this Law or another legal provision permits the processing thereof or
2. the person concerned has given his consent.
Consent shall be given in writing except where another form of consent is appropriate owing to special circumstances. Where consent is given in writing together with other declarations, the person concerned shall be informed thereof in writing.

Section 4 Rights of the person concerned
Subject to the provisions of this Law every person shall be entitled to
1. information on stored data concerning him;
2. correction of any incorrect stored data concerning him;
3. blocking of stored data concerning him where their accuracy or inaccuracy cannot be established or where the original requirements for their storage no longer apply;
4. erasure of stored data concerning him where such storage was inadmissible or - as an option to the right to the blocking of data - where the original requirements for storage no longer apply.

Section 5 Confidentiality
(1) Persons engaged in data processing and referred to in Section 1 (2) or acting on behalf of the persons or establishments referred to therein shall not, without authorization, process, communicate, grant access to or otherwise use protected personal data for any purpose other than that of the legitimate accomplishment of their task.
(2) On taking up their duties, such persons shall be required to make an undertaking to abide by paragraph 1. This undertaking shall continue to be valid after termination of their activity.

Section 6 Technical and organizational measures
(1) Persons processing personal data referred to in Section 1 (2) or acting on behalf of the persons or establishments referred to therein shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Law. Measures shall be required only if the cost involved is reasonable in relation to the desired level of protection.³
(2) The Federal Government is empowered to issue orders, with the approval of the Bundesrat, adjusting the requirements set out in the Annex to the current state of the art and organization. For the purposes of this Law the state of the art and organization shall be the level of

³ See also Annex at the end of the translation.
development of progressive procedures, systems or methods of operation which appears to ensure the practical suitability of a measure to guarantee the implementation of this Law. In determining the state of the art and organization reference shall in particular be made to comparable procedures, systems or methods of operation which have already been successfully employed.

PART II Data processing by public authorities and other public establishments

Section 7 Field of application
(1) The provisions of this Part shall apply to public authorities and other public establishments of the Federal Government or of public-law entities, institutions and foundations directly owned, employed or operated by the Federal Government and associations of such entities, institutions and foundations. However, only Sections 15 to 21 of this Part shall apply to public-law undertakings participating in competition.
(2) Insofar as data protection is not governed by Land law, the provisions of this Part, with the exception of Sections 15 to 21 shall also apply to
   1. public authorities and other public establishments of the “Lander”, of communes and associations of communes and of other public-law entities subject to the supervision of the Land and associations thereof insofar as they implement Federal law;
   2. public authorities and other public establishments of the “Lander” insofar as they act as organs for the administration of justice, except in administrative matters.

The provisions of this Part shall not apply to public law undertakings which participate in competition, provided that they meet the requirements set out in the first sentence of paragraph 1 above.
(3) By way of derogation from paragraphs (1) and (2), Sections 23 to 27, and not Sections 9 to 14, shall apply mutatis mutandis where data processing concerns a previous, existing or future legal relationship governed by labour law.

Section 8 Processing of personal data on behalf of third parties
(1) The provisions of this Part shall apply to the establishments referred to in Section 7 (1) and (2) where personal data are processed on their behalf by other persons or establishments. Such persons or establishments shall be carefully selected, with particular account to be taken of the suitability of the technical and organizational measures taken by them (Section 6 (1)).
(2) With the exception of Sections 15 to 21, the provisions of this part shall not apply to the establishments referred to in Section 7 (1) and (2), where they process personal data on behalf of third parties. In such cases the processing of personal data shall be permissible in each of the phases specified in Section 1 (1) only as instructed by the principal.
(3) Sections 15 to 21 shall apply mutatis mutandis to legal entities, companies and other private-law associations in which the Federal Government or a public-law entity, institution or foundation directly owned, employed or operated by the Federal Government, holds the majority of the shares or has a voting majority, insofar as such entities or associations act on behalf of third parties in the cases set out in the first sentence of paragraph 1.

Section 9 Storage and modification of data
(1) The storage and modification of personal data shall be permissible where necessary for the legitimate accomplishment of the tasks for which the storage unit is competent.
(2) Where data are collected from the person concerned on the basis of a legal provision, his attention shall be drawn thereto, and in all other cases he shall be informed that he is not obliged to provide the data.

Section 10 Communication of data within the public sector
(1) The communication of personal data to public authorities and other public establishments shall be permissible where it is necessary for the legitimate accomplishment of the tasks for which the communicating unit or the recipient is competent. Where the personal data are subject to professional or special official secrecy (Section 45, second sentence, paragraph 1, third sentence) and where they have been communicated to the communicating unit by the person committed to secrecy in the performance of his professional or official duty, the permissibility of communication shall also be subject to the condition that the recipient requires the data for the accomplishment of the same purpose as that for which the communicating unit obtained them.

(2) The communication of personal data to establishments of public-law religious societies is permissible by application, mutatis mutandis, of the provisions concerning the communication of data to public authorities and other public establishments, provided that adequate data protection measures are taken by the recipient.

Section 11 Communication of data to establishments outside the public sector

The communication of personal data to persons and other establishments than those specified in Section 10 is permissible where it is necessary for the legitimate accomplishment of tasks for which the communicating unit is competent or where the recipient can demonstrate convincingly that his interest in the data to be communicated is justified and the communication of the data does not harm interests of the person concerned that warrant protection. Where the personal data are subject to professional or special official secrecy (Section 45, second sentence, paragraph 1, third sentence) and where they have been communicated to the communicating unit by the person committed to secrecy in the performance of his professional or official duty, the permissibility of communication shall also be subject to the requirement that the same conditions are met under which the person committed to secrecy would be permitted to communicate them. As regards the communication of data to public authorities and other establishments not governed by this Law and to supranational and international establishments, the first and second sentences shall apply subject to the laws and agreements applicable to such communication.

Section 12 Public notices concerning stored data

(1) Immediately following the initial storage public authorities and other official establishments shall announce in the relevant official bulletin for their sector

1. the type of personal data stored by them or on their behalf,
2. the tasks for which knowledge of these data is required,
3. the group of persons concerned,
4. the establishments to which they regularly communicate personal data, and
5. the type of data to be communicated.

On request previous notices shall be made available to the person concerned.

(2) Paragraph 1 shall not apply to

1. the authorities responsible for the protection of the constitution, the Federal Intelligence Service, the Military Counterintelligence Service and other departments of the Federal Ministry of Defence in matters involving the security of the Federal Republic, the Federal Criminal Investigation Office, the departments of the Public Prosecutor, and the police, and Federal and Land financial authorities, insofar as they store personal data, for the purpose of supervision and examination, in data files in the performance of their legitimate duties under the Tax Code;
2. personal data which are blocked in accordance with Section 14 (2), second sentence, because they may not be erased, pursuant to Section 14 (3), first sentence, owing to the existence of legal provisions regarding their retention;
3. registers prescribed by law or other data files the maintenance of which is required by legal or published administrative provisions, provided that the type of personal data stored in them, the tasks for which knowledge of these data is required, the persons concerned, the establishments to which personal data are regularly communicated and
the type of data to be communicated are specified in legal or published administrative provisions.

(3) The Federal Government is empowered to issue regulations, for which the approval of the Bundesrat is not required, defining the bulletin and the publication procedure to be used by the public authorities and other public establishments referred to in Section 7 (1), first sentence. The Land governments are authorized to issue regulations defining the bulletin and publication procedure to be used by the public authorities and other public establishments referred to in Section 7 (2), first sentence.

Section 13 Provisions of information to the person concerned
(1) The person concerned shall, at his request, be provided with information on stored data concerning him. The request should describe in detail the type of personal data on which information is to be provided. The storage unit shall exercise due discretion in determining the procedure for providing such information and, in particular, the form in which it is provided.
(2) Paragraph 1 shall not apply in the cases specified under Section 12 (2), subparagraphs 1 and 2.
(3) No information shall be provided:
1. if the information would be prejudicial to the legitimate accomplishment of the tasks for which the storage unit is competent;
2. if the information would be prejudicial to public security or order or otherwise to the disadvantage of the Federal Republic or of a Land;
3. if the personal data or the fact that they are being stored must be kept secret in accordance with a legal regulation or by reason of their nature, in particular by reason of an overriding and justified interest of a third person;
4. if the information concerns the communication of personal data to the public authorities referred to in Section 12 (2), subparagraph 1.
(4) A fee shall be payable for the provision of information. The Federal Government is empowered to issue regulations, with the approval of the Bundesrat, determining the services for which fees are payable, the amount of such fees and granting exemptions therefrom. Fees may only be charged to cover administrative expenditure arising directly from such official action. In particular, fees may be waived in cases where, owing to special circumstances, it may justifiably be assumed that stored personal data are inaccurate or that their storage was inadmissible or where the information provided has led to the correction or erasure of stored personal data. In other cases the Law on Administrative Expenses shall apply.

Section 14 Correction, blocking and erasure of data
(1) Incorrect personal data shall be corrected.
(2) Personal data shall be blocked if their accuracy is disputed by the person concerned and where neither their accuracy nor their inaccuracy can be established. They shall also be blocked when they are no longer required for the accomplishment of the tasks for which the storage unit is competent. Blocked data shall be marked appropriately and may no longer be processed, and in particular may not be communicated, or otherwise used except where they are indispensable for scientific purposes, for use as evidence or for other reasons in the overriding interests of the storage unit or a third person or where the person concerned has consented to their use.
(3) Personal data may be erased when knowledge thereof is no longer required by the storage unit for the legitimate accomplishment of the tasks for which it is competent, and where there is no reason to assume that personal interests warranting protection would be harmed by such erasure. They shall be erased when their storage was inadmissible or when the person concerned so requests pursuant to paragraph 2, second sentence.

Section 15 Implementation of data protection in the Federal Administration
The supreme federal authorities, the managing board of the German Federal Railways and the public-law entities, institutions and foundations directly responsible owned, employed or
operated by the Federal Government over which only lawful supervision is exercised by a supreme
federal authority, shall ensure that this Law and other legal provisions concerning data protection
are implemented in their respective spheres of activity. In particular they shall ensure that
1. a record is kept of the type of personal data stored, of the tasks for which knowledge of
those data is required and of particular recipients of these data and
2. data processing programmes by means of which personal data are to be processed, are
properly used.

Section 16 General administrative provisions
The supreme federal authorities and the managing board of the German Federal Railways shall lay
down for their respective areas of activity general administrative provisions, which shall govern
the implementation of this Law, with account taken of the specific circumstances of each area of
activity and the specific data protection requirements arising therefrom.

Section 17 Appointment of a federal commissary for data protection
(1) A federal commissary for data protection shall be appointed by the Federal President on a
proposal from the Federal Government. He shall be at least 35 years old at the time of his
appointment.
(2) The federal commissary shall swear the following oath in the presence of the Federal Minister
of the interior:
"I swear to do everything in my power to further the well-being of the German people, to
protect it from harm and to defend the Constitution and the laws of the Federal Republic,
to perform my duties conscientiously and to exercise justice in all my dealings, so help me
God."
The reference to God may be omitted from the oath.
(3) The term of office of the federal commissary shall be five years and may be renewed once.
(4) The federal commissary shall, as directed by this Law, have public-law official status with
respect to the Federal Government. He shall be independent in the performance of his duties and
subject to the law only. He shall be subject to the lawful supervision of the Federal Government.
(5) The federal commissary shall be installed at the Federal Ministry of the Interior. He shall report
to the Federal Minister of the Interior. The federal commissary shall be provided with the human
and material resources necessary for the accomplishment of his tasks; these shall be shown in a
separate chapter of the budget of the Federal Ministry of the Interior.
(6) If the federal commissary is temporarily prevented from performing his duties, the Federal
Minister of the Interior may appoint a substitute to perform such duties. The federal commissary
shall be consulted on such appointment.

Section 18 Legal status of the federal commissary for data protection
(1) The mandate of the federal commissary for data protection shall commence on delivery of the
certificate of appointment. It shall end
  1. on expiry of his term of office,
  2. on his dismissal.
The Federal President shall dismiss the federal commissary at the latter's request, or on a proposal
by the Federal Government when there are reasons, in the opinion of an established judge, for
dismissal from the service. In the event of termination of office the federal commissary shall
receive a document signed by the Federal President. Dismissal shall be effective on delivery of
this document. If the Federal Minister of the Interior so requests, the federal commissary shall
be obliged to continue his work until his successor has been appointed.
(2) The federal commissary shall not hold any other paid office or pursue any gainful activity or
occupation in addition to his official duties and shall not belong to the management, supervisory
board or board of directors of a profit-making enterprise, or a government or a legislative body of
the Federal Republic or a Land. He may not deliver extrajudicial opinions in exchange for payment.
(3) The federal commissary shall inform the Federal Minister of the Interior of any gift he receives in the performance of his duties. The Federal Minister of the Interior shall decide how such gifts shall be used.

(4) The federal commissary shall be obliged, even after termination of his service, to maintain secrecy concerning information of which he has knowledge by reason of his duties. This shall not apply to communications made in the normal course of duties or concerning facts which are common knowledge or are not sufficiently important to warrant confidential treatment. The federal commissary may not, even after leaving the service, make any pronouncements or statements either in or out of court concerning such matters without the consent of the Federal Minister of the Interior. This provision shall not, however, affect his duty by law to report criminal offences and to take action to uphold the free democratic fundamental order whenever it is jeopardized.

(5) Consent to give testimony as a witness shall be refused only when such testimony would be to the disadvantage of the Federal Republic or a German Land or seriously jeopardize or impede the performance of public tasks. Consent to deliver an opinion may be refused where it would be against the interests of the service. Section 28 of the Law on the Federal Constitutional Court as published on 3 February 1971 (Federal Law Gazette I, p. 105), amended by the Law to Introduce the Penal Code of 2 March 1974 (Federal Law Gazette I, p. 409) shall remain unaffected hereby.

(6) From the beginning of the calendar month in which he commences his duties until the end of the calendar month in which he terminates his duties, or in the event of the application of paragraph 1, sixth sentence, until the end of the month in which activities cease, he shall receive the remuneration of a grade B 9 federal official. The Federal Law on Travel Expenses and the Federal Law on Removal Expenses shall apply mutatis mutandis. In addition, Sections 13 to 20 of the Law on Federal Ministers as published on 27 July 1971 (Federal Law Gazette I, p. 1166), last amended by the Seventh Law on the Amendment of the Regulations on Officials and Remunerations of 20 December 1974 (Federal Law Gazette I, p. 3716), shall apply, except that the period of office of two years provided for in Section 15 (1) of the Law on Federal Ministers shall be replaced by a period of office of 5 years.

Section 19 Duties of the federal commissary for data protection

(1) The federal commissary for data protection shall ensure that the provisions of this Law and other provisions concerning data protection are observed by the public authorities and other public establishments of the Federal Republic referred to in Section 7 (1), with the exception of the courts where these do not deal with administrative matters. For this purpose he may make recommendations for the improvement of data protection. In particular, he may advise the Federal Government and individual ministers and also the other public authorities referred to in Section 7 (1) and other establishments in matters of data protection.

(2) When so requested by the German Bundestag or the Federal Government, the federal commissary shall draw up opinions and reports. In addition, he shall submit an activity report to the German Bundestag annually, the first such report to be submitted on 1 January 1979. When so requested by the German Bundestag, the Committee on Petitions of the German Bundestag or the Federal Government, the federal commissary may also investigate references to matters and events directly related to his sphere of activities. The commissary may at any time consult the German Bundestag.

(3) The public authorities and other establishments referred to in paragraph 1, first sentence, shall assist the federal commissary and his assistants in the accomplishment of their tasks. In particular, the federal commissary and his assistants shall be

1. provided with information in response to their questions and granted access to documents and files related to the processing of personal data, and especially to stored data in storage and to data processing programmes;
2. granted access to all offices at all times.

The first and second sentences shall apply to the federal authorities referred to in Section 12 (2),
subsection 1, except that assistance shall be granted only to the federal commissary and those of
his assistants specifically named by him in writing. The second sentence shall not apply to
the federal authorities referred to in Section 12 (2) subsection 1 where the competent
supreme federal authority decides in the case concerned that the inspection of documents and
files would jeopardize the security of the Federal Republic or of a Land.
(4) The federal commissary shall keep a register of automatically operated data files in which
personal data are stored. The register shall be open to be inspected by any person. The public
authorities and other establishments referred to in paragraph 1, first sentence, shall register with
the federal commissary the data files automatically operated by them. The Federal Office for the
Protection of the Constitution, the Federal Intelligence Service and the Military
Counterintelligence Service shall be exempt from this obligation. A special register shall be kept of
the data files of the other federal authorities referred to in Section 12 (2), Subparagraph 1. This
register shall be restricted to type and purpose. The second sentence shall not apply to these
registers. The Federal Minister of the Interior shall issue a regulation providing further details in
this regard.
(5) The federal commissary shall strive to achieve cooperation with the public authorities and
other public establishments responsible for ensuring that the provisions on data protection are
observed in the Landers and also with the supervisory authorities provided for in Section 30.

Section 20 Complaints lodged by the federal commissary for data protection
(1) Should the federal commissary for data protection discover infringements against the
provisions of this Law or against other data protection regulations, or other irregularities in the
processing of personal data, he shall submit a complaint
1. in the case of the Federal Administration, to the competent supreme federal authority;
2. in the case of the Federal Railways, to the managing board;
3. in the case of public-law entities, institutions and foundations directly owned, employed or
operated by the Federal Government and in the case of associations of such entities, institutions
and foundations, to the managing board or the relevant representative body, requesting them to
pronounce on the matter by a date which he shall determine. In the case of the establishments
referred to in subparagraph 3 the federal commissary shall at the same time inform the
competent supervisory authority.
(2) The federal commissary may refrain from making a complaint or requesting an opinion from
the establishment concerned if the irregularities involved are not significant.
(3) The federal commissary may submit with his complaint proposals for the elimination of the
irregularities concerned and other improvements in data protection.
(4) The opinion to be delivered pursuant to paragraph 1 should also describe the measures taken
as a result of the federal commissary’s complaint. The establishments referred to in paragraph 1,
subparagraph 3, shall submit to the competent supervisory authority a copy of the opinion
communicated to the federal commissary.

Section 21 Appeals to the federal commissary for data protection
Any person may apply to the federal commissary for data protection if he believes that his rights
have been violated as a result of his personal data being processed by the public authorities or
other public establishments of the Federal Republic referred to in Section 7 (1), with the exception
of the courts, provided they do not deal with administrative matters.

PART III Data processing by private establishments for their own purposes.

Section 22 Field of application
(1) The provisions of this part shall apply to physical and legal persons, companies, and other
private-law associations which process protected personal data as an aid to the achievement of
their aims or to the purpose of their activities. These provisions, with the exception of Sections 28 to 30, shall also apply, in accordance with the first sentence, to public-law undertakings which participate in competition, provided that they meet the requirements set out in Section 7 (1), first sentence, or Section 7 (2), first sentence, subparagraph 1.

(2) The provisions of this part shall also apply to the persons, companies, and other associations referred to in paragraph 1 where personal data are processed by other persons or establishments on their behalf. Such persons or establishments shall be carefully selected, with particular account taken of the suitability of the technical and organizational measures taken by them (Section 6 (1)).

(3) The provisions of this part shall not apply to the persons, companies, and other associations mentioned in paragraph 1 which carry out public administration work.

Section 23 Storage of data
The storage of personal data is permissible if it serves the purpose of a contractual relationship or a quasicontractual relationship of trust with the person concerned or insofar as it is necessary in order to safeguard the justified interests of the storage unit and provided there is no reason to suppose that interests of the person concerned warranting protection will be harmed. By way of derogation from the first sentence storage by non-automatic methods shall be permissible provided that the data are derived directly from generally accessible sources.

Section 24 Communication of data
(1) The communication of personal data shall be permissible if it serves the purpose of a contractual relationship or quasi-contractual relationship of trust with the person concerned or insofar as it is necessary in order to safeguard the justified interests of the communicating unit or of a third party or of the general public and provided that interests of the person concerned warranting protection are not harmed thereby. Personal data which are subject to professional or special official secrecy (Section 45, second sentence, paragraph 1, third sentence) and which have been communicated by the person committed to secrecy in the performance of his professional or official duty may not be passed on by the recipient.

(2) By way of derogation from paragraph 1, the communication of data, in lists or otherwise compiled concerning members of a group of persons shall be permissible where this is confined to

1. name
2. title, academic qualifications
3. date of birth
4. occupation, trade or business activities
5. address
6. telephone number

and where there is no reason to suppose that interests of the person concerned warranting protection would be harmed thereby. No data other than those mentioned in the preceding sentence may be communicated for the purpose of indicating membership of the person concerned to a group of persons.

Section 25 Modification of data
The modification of personal data is permissible if it serves the purpose of a contractual relationship or quasi-contractual relationship of trust with the person concerned or insofar as it is necessary in order to safeguard the justified interests of the storage unit and provided that there is no reason to suppose that interests of the person concerned warranting protection will be harmed thereby.

Section 26 Provision of information to the person concerned
(1) The person concerned shall be informed when data concerning his person are stored for the first time, unless he has gained knowledge of such storage by other means.
(2) The person concerned may demand information on stored data relating to his person. Where the data are processed automatically, the person concerned may also request information on the persons and establishments to which his data are regularly communicated. He should give details of the type of personal data on which information is to be provided. The information shall be provided in writing unless by reason of special circumstances, some other form of communication is appropriate.

(3) A fee may be charged for the provision of information. The fee may not exceed the costs directly attributable to the provision of information. No fee may be charged in cases where special circumstances give rise to the assumption that stored personal data are inaccurate or that their storage was inadmissible, or where the information has revealed that the personal data should be corrected or, subject to Section 27 (3), second sentence, first phrase, erased.

(4) Paragraphs 1 and 2 shall not apply where
1. the disclosure of personal data would substantially undermine the aims of the storage unit or the purpose of its activities and where the justified interests of the person concerned would not be harmed.
2. the competent public establishment has determined that the disclosure of personal data by the storage unit would constitute a threat to public security or order or otherwise be to the disadvantage of the Federal Republic or of a Land;
3. the personal data must be kept secret in accordance with a legal provision or by reason of their nature, in particular by reason of the overriding justified interests of a third person;
4. the personal data are derived directly from generally accessible sources;
5. the personal data are blocked in accordance with Section 27 (2), second sentence, because they may not be erased in accordance with Section 27 (3), first sentence, because of legal, statutory or contractual provisions on retention.

Section 27 Correction, blocking and erasure of data
(1) Incorrect personal data shall be corrected.
(2) Personal data shall be blocked if their accuracy is disputed by the person concerned and where neither their accuracy nor their inaccuracy can be established. They shall also be blocked when knowledge thereof is no longer required to achieve the purpose for which they were originally stored. The provisions concerning the procedure and the legal consequences of blocking laid down in Section 14 (2), third sentence, shall apply mutatis mutandis.
(3) Personal data may be erased when knowledge thereof is no longer required to achieve the purpose for which they were originally stored, and where there is no reason to suppose that interests of the person concerned that warrant protection would be harmed by such erasure. They shall be erased when their storage was inadmissible or when the person concerned so requests, pursuant to paragraph 2, second sentence. Data concerning health, criminal offences, offences against public order, and religious or political opinions shall be erased where they cannot be proved to be accurate by the storage unit.

Section 28 Appointment of a commissary for data protection
(1) The persons, companies and other associations referred to in Section 22 (1) and (2) which process personal data automatically and regularly employ at least five employees permanently for this purpose, shall appoint in writing a commissary for data protection within one month of the commencement of their activities. The same shall apply where personal data are processed by other means, provided that at least twenty employees are permanently employed for this purpose.
(2) Only persons who possess the specialized knowledge and demonstrate the reliability necessary for the accomplishment of the tasks concerned may be appointed to the post of a commissary for data protection.
(3) The commissary for data protection shall be directly subordinate to the owner, managing board, managing director or other lawfully or constitutionally appointed manager. He shall be free to use his specialized knowledge in the area of data protection at his own discretion. He shall suffer no disadvantage through the performance of his duties.

(4) The commissary for data protection shall be assisted in the performance of his duties by the persons, companies or other associations required to appoint him pursuant to paragraph 1.

Section 29 Duties of the commissary for data protection
The commissary for data protection shall be responsible for ensuring that this Law and other provisions concerning data protection are observed. For this purpose he may apply to the supervisory authority (Section 30) in cases of doubt. In particular he shall
1. keep a record of the types of personal data stored and of the purposes and aims for which knowledge of these data is required, of regular recipients of such data and of the type of automatic data processing facilities used;
2. ensure that the data-processing programmes by means of which personal data are to be processed are used properly;
3. take suitable steps to inform the persons employed in the processing of personal data of the provisions of this law and other provisions concerning data protection, with particular reference to the situation prevailing in this area and the special requirements as to the protection of data arising therefrom;
4. assist and advise in the selection of persons to be employed in the processing of personal data.

Section 30 Supervisory authority
(1) The supervisory authority responsible pursuant to Land Law shall ensure that this Law and other provisions concerning data protection within the field of application of this Part are observed in individual cases where a person concerned submits evidence that his rights have been violated during the processing of his personal data by one of the persons, companies or other associations referred to in Section 22 (1) and (2). It shall render the commissary for data protection any assistance he may request (Section 29 (1) second sentence).
(2) The persons, companies and other associations referred to in Section 22 (1) and (2) and the persons responsible for their management shall provide the supervisory authority on request and without delay the information necessary for the performance of its tasks. A person obliged to provide information may refuse to do so where he would expose himself or one of the persons designated in Section 383 (1), subparagraphs 1 to 3 of the Code of Civil Procedure to the danger of criminal prosecution or of proceedings under the Law concerning Administrative offences.
(3) The persons appointed by the supervisory authority to exercise control are authorized, insofar as it is necessary for the accomplishment of the tasks devolving upon the supervisory authority, to enter the property and premises of the establishment to carry out checks and inspections and to inspect business documents, and in particular the record to be kept pursuant to Section 29, paragraph 1. by the commissary for data protection, the personal data stored and the data-processing programs. The persons obliged to provide information shall permit such measures. The fundamental right of the inviolability of the home (Article 13 of the Constitution) shall be correspondingly restricted.
(4) The Industrial Code shall continue to apply to commercial firms subject to the provisions of this Part.
(5) The Land governments or the establishments authorized by them shall designate the supervisory authorities responsible for supervising the implementation of data protection within the field of application of this Part.

PART IV Commercial data processing by private establishments for others
Section 31 Field of application
(1) The following sections shall apply to physical and legal persons, companies and other private-law associations and to public-law undertakings which participate in competition provided that they meet the requirements set out in Section 7 (1), first sentence of Section 7 (2), first sentence, subparagraph 1:

1. Section 32 to 35, insofar as such establishments store for the purposes of communication and communicate protected personal data in the normal course of business, irrespective of whether the data are modified before communication;
2. Section 36, insofar as such establishments store for the purposes of modification protected personal data in the normal course of business, modify them in such a way that they no longer relate to a specific person or render such a person recognizable, and communicate them in this form;
3. Section 37, insofar as such establishments, in processing protected personal data in the normal course of business, act as service-rendering undertakings on behalf of third parties.

In addition, Sections 38 to 40 shall apply to physical and legal persons, companies and other private-law associations. The second sentence shall not apply to legal persons, companies and other private-law associations in which the majority of shares or the majority of votes are held by public authorities, provided that such persons or associations, in processing protected personal data in the normal course of business, act as service-rendering undertakings on behalf of public authorities or other public establishments. Section 8 (3) shall remain unaffected by the foregoing provision.

(2) The provisions contained in paragraph 1 shall apply to the persons, companies and other associations referred to therein even where the processing of personal data is carried out on their behalf by other persons or establishments. Such persons or establishments shall be carefully selected, with particular account taken of the suitability of the technical and organizational measures taken by them (Section 6 (1)).

Section 32 Storage and communication of data
(1) The storage of personal data shall be permissible provided that there is no reason to assume that interests of the person concerned warranting protection will be harmed thereby. By way of derogation from the first sentence storage shall be permissible provided that the data are derived directly form generally accessible sources.

(2) The communication of personal data shall be permissible if the recipient demonstrates convincingly a justified interest in having knowledge thereof. The reasons for the existence of a justified interest and the means used for its justification shall be recorded.

(3) By way of derogation from paragraph 2, first sentence the communication of data, assembled in lists or otherwise compiled concerning members of a group of persons shall be permissible where this is confined to name, title, academic qualifications, address and. one item regarding the membership of the person concerned of the group of persons and provided there is no reason to suppose that interests of the person concerned warranting protection would be harmed thereby.

Section 33 Modification of data
The modification of personal data shall be permissible provided that interests of the person concerned warranting protection are not harmed thereby.

Section 34 Provision of information to the person concerned
(1) When personal data on the person concerned are communicated for the first time, he shall be informed of their storage unless he gains knowledge thereof by other means. Sentence 1 shall not apply to communications made pursuant to Section 32 (3).

(2) The person concerned may request information concerning stored data relating to his person. Where the data are processed automatically, the person concerned may also request information
concerning the persons or establishments to which his data are regularly communicated. The information shall be given in writing unless, by reason of special circumstances some other form of notification is appropriate.

(3) A fee may be charged for the provision of information, but may not exceed the costs directly attributable to the provision of information. No fee may be charged in cases where it may justifiably be assumed, owing to special circumstances, that stored personal data are inaccurate or that their storage was inadmissible, or where the information has revealed that the personal data should be corrected, or, subject to Section 35 (3), second sentence, first phrase, erased.

(4) Paragraphs 1 and 2 shall not apply where the disclosure of personal data would harm the overriding justified interests of a third person, or where it has been ascertained by the competent public establishment on consulting the storage unit that disclosure would constitute a threat to public safety or order or otherwise be to the disadvantage of the Federal Republic or of a Land.

Section 35 Correction, blocking and erasure of data

(1) Incorrect personal data shall be corrected.

(2) Personal data shall be blocked if their accuracy is disputed by the person concerned and where neither their accuracy nor their inaccuracy can be established. They shall also be blocked at the end of the fifth calendar year after being stored. The provisions concerning the procedure and the legal consequences of blocking as set out in Section 14 (2), third sentence, shall apply mutatis mutandis.

(3) Personal data may be erased when there is no reason to suppose that interests of the person concerned warranting protection would be harmed thereby. They shall be erased when their storage was inadmissible or where the person concerned so demands pursuant to paragraph 2, second sentence. Data concerning health, criminal offences, offences against public order and religious or political opinions shall be erased if the storage unit cannot prove them to be accurate.

Section 36 Processing of personal data for the purposes of communication in anonymous form

(1) The persons, companies and other associations of persons referred to in Section 31 (1), subparagraph 2, shall render stored personal data anonymous. The features for modifying anonymous data in such a way that they relate to a specific person or permit such a person to be identified, shall be stored separately. Such features may no longer be stored with anonymous data unless the use of these data made possible by such features is necessary to achieve the aims for which the data were stored or for scientific purposes.

(2) Sections 33 and 35 (3), first sentence and second sentence, first phrase, shall apply mutatis mutandis to the modification and erasure of personal data.

(3) In the case of automatic data processing appropriate arrangements shall be made to ensure the implementation of the measures provided for in paragraph 1.

Section 37 Processing of personal data on behalf of third parties

The persons, companies and other groups of persons referred to in Section 31 (1), subparagraph 3, shall be permitted to process personal data in each of the phases referred to in Section 1 (1) only as instructed by the principal.

Section 38 Commissary for data protection

The persons, companies and other associations of persons referred to in Section 31 shall appoint a commissary for data protection. The provisions of Sections 28 and 29 concerning the commissary for data protection shall apply mutatis mutandis.

Section 39 Obligatory notification

(1) The persons, companies and other associations of persons referred to in Section 31 and their subsidiary branches and dependent agencies shall notify the competent supervisory authority of the commencement of other activities within one month.
(2) The following particulars shall be submitted for entry in the register kept by the supervisory
authority:
1. name or firm of the establishment,
2. proprietor, managing boards, managers or other legally or constitutionally appointed directors
and persons responsible for data processing operations,
3. address,
4. aims or purpose of the activities of the establishment and of the data processing,
5. type of automatic data processing facilities used,
6. name of the commissary for data protection,
7. type of personal data stored by the establishment or on its behalf,
8. in the event of regular communication of personal data, recipients and type of data
communicated.
(3) Paragraph 1 shall apply mutatis mutandis to the termination of the activities and to the
modification of the particulars provided in accordance with subparagraph 2.

Section 40 Supervisory authority
(1) The supervisory authority competent in accordance with Land Law shall ensure that this Law
and other provisions concerning data protection within the field of application of this Part are
observed; in particular, it shall also perform the tasks referred to in Section 30 (1). It shall keep the
register of the establishments required to register pursuant to Section 33 (1), the register may be
inspected by any person.
(2) The remaining provisions concerning the supervisory authority contained in Section 30 (2) to
(5) shall apply mutatis mutandis.

PART V Penalties and fines

Section 41 Offences
(1) Any person who, where not authorized to do so by this law,
1. communicates or modifies or
2. retrieves or procures from data files in sealed containers, protected confidential
personal data shall be liable to a term of imprisonment not exceeding one year, or to a
fine.
(2) Where the offender commits his offence in exchange for payment or with the intention of
enriching himself or another person or of harming another person, he shall be liable to a term of
imprisonment not exceeding two years, or to a fine.
(3) Such offences shall be prosecuted only if a complaint is filed.

Section 42 Administrative Offences
(1) An administrative offence shall be deemed to be committed by any person who, whether
intentionally or through negligence,
1. contrary to Section 26 (1) and Section 34 (1), fails to inform the person concerned,
2. contrary to Section 28 (1) and Section 38 in conjunction with Section 28 (1), fails to
appoint a commissary for data protection or fails to do so within the prescribed time-limit,
3. contrary to Section 32 (2), second sentence, fails to record the reasons or means ref-
erred to in that section,
4. contrary to Section 39 (1) or (3), fails to notify the competent supervisory authority or
fails to do so within the prescribed time-limit or, contrary to Section 39 (2) or (3) fails,
when registering, to provide the required particulars, or provides incorrect or incomplete
particulars, 5. contrary to Section 30 (2), first sentence, and Section 40 (2) in conjunction
with Section 30
(2), first sentence gives information not correct or not complete, or fails to provide
information, or fails to do so within the prescribed time limit or, contrary to Section 40 (2)
in conjunction with Section 30 (3), second sentence, refuses to grant access to property or premises or refuses to permit checks or inspections or the inspection of documents.

(2) Persons committing such an administrative offence shall be liable to a fine not exceeding DM 50,000.

PART VI Transitional and final provisions

Section 43 Transitional provisions

(1) Public notices concerning personal data (Section 12) which had already been stored prior to the entry into force of this Law, shall appear within one year of the entry into force of this Law. (2) The obligations referred to in Section 28 (1) and Section 30 in conjunction with Section 28 (1) and Section 39 (1) shall enter into force at the same time as the Law in respect of persons, companies and other associations of persons processing personal data at the time of entry into force of this Law.

(3) Where data on the person concerned have been stored prior to the entry into force of the Law, the person concerned shall be informed thereof pursuant to Section 26 (1) when the first communication of the data after the entry into force of the Law has taken place.

(4) Where stored data on the person concerned were already communicated prior to the entry into force of the Law, the person concerned shall be informed of their storage pursuant to Section 34 (1) when the first communication of the data after the entry into force of the Law has taken place.

Section 44 Application of the Law on Administrative Procedures

For the purposes of implementing this Law, the Law on Administrative Procedures shall also be applied insofar as such implementation is the responsibility of the Lander.

Section 45 Provisions which continue to be valid

Where special provisions of the Federal Republic are applicable to personal data stored in data files, they shall take precedence over the provisions of this Law. Such provisions include in particular:

1. provisions concerning the confidentiality of information acquired in the performance of duties or otherwise in the exercise of an occupation, e. g., Section 12 of the Law on Statistics for Federal purposes of 3 September, 1953 (Federal Law Gazette I, p. 1314), last amended by Law on 3 May, 1974 (Federal Law Gazette I, p. 469), Section 30 of the Tax Code, Section 9 of the Banking Law as published with the amendment of 3 May 1976 (Federal Law Gazette I, p. 1121), Section 5 and 6 of the Law on the Postal Service and Section 10 and 11 of the Law on the Telecommunications Facilities;

2. provisions concerning the right to withhold testimony and information for personal or professional reasons in judicial and administrative proceedings, e. g., Sections 52 to 55 of the Code of Criminal Procedure, Sections 383 and 384 of the Code of Civil Procedure and Sections 102 and 105 of the Tax Code;

3. provisions concerning the obligation to store data or the limitation or prohibition of storage, communication or publication of individual particulars concerning persons, e. g., Section 161 of the Code of Criminal Procedure, Sections 20 and 22 of the Law to Promote Employment of 25 June 1969 (Federal Law Gazette I, p. 582) last amended by Law of 16 March 1976 (Federal Law Gazette I, p. 581), and Section 49 of the Law on the Federal Central Register;

4. provisions concerning restrictions on the inspection of documents by third parties, e. g., Section 61 (2) and (3) of the Law on Family Status, Section 36 of the Law on Administrative Procedures concerning Aid to War Victims as published with the announcement of 6 May 1976 (Federal Law Gazette I, p. 1169);

5. provisions concerning the inspection by a civil servant or an employee of documents concerning his person e. g. Section 90 of the Federal Officials Law and Section 83 of the Law on the
Constitution of Enterprises;
6. provisions concerning the duty of authorities to provide citizens with information on stored
data concerning them, e. g., Section 1325 of the Reich Insurance Code, Section 104 of the
Salaried Employees' Insurance Law and Section 108 (h) of the Reich Law on Miners' Unions;
7. provisions concerning the communication, correction and erasure of personal data recorded in
public registers e. g., Section 19, 23, 27 (2), 31, 37 (1), 39 to 47 and 58 of the Law on the
Federal Central Register, Section 30 of the Road Traffic Law, Section 13 (a) of the Road Transport
Licensing Order and Section 12 and the Part II of the Land Register Code;
8. provisions concerning the obligation to process personal data during accounting, including
bookkeeping and other recording operations, e. g., Sections 38 to 40 and Sections 42 to 47
of the Commercial Code, Sections 140 to 148 of the Tax Code, Section 8 of Order on Price
Laws No. 30/5 3 concerning prices in the case of public works contracts of 21 November 1953
(Federal Journal No. 244) and Section 71 of the Federal Budget Order.
The obligation to keep the professional secrets referred to in Section 203 (1) of the Penal Code,
e.g., medical secrets, shall not be affected hereby.

Section 46 Berlin clause
In accordance with Section 13 (1) of the Third Transference Law of 4 January 1952 (Federal Law
Gazette I P. 1) this Law shall also apply in the Land of Berlin. Orders issued on the basis Law shall
apply in the Land of Berlin pursuant to Section 14 of the Third Transference Law.

Section 47 Entry into force
This Law shall enter into force on 1 January 1978.
By way of derogation:
1. Section 12 (3), Section 13 (4), Section 16 and Section 19 (4), eighth sentence, shall enter into
force on the day following the promulgation of the Law;
2. Sections 17, 18, 28 and 38 shall enter into force on 1 July 1977;
3. Section 6 and the Annex to Section 6 (1), first sentence, shall enter into force on 1 January 1979.

Annex to Section 6 (1), first sentence
Where personal data are processed automatically appropriate measures suited to the type of
personal data to be protected, shall be taken to ensure observance of the provisions of this Law:
1. Unauthorized persons shall be refused to admission to data processing facilities which process
personal data (admission control);
2. Persons employed in the processing of personal data shall be prevented from removing storage
media without authorization (leakage control);
3. Unauthorized input into the storage and the unauthorized gaining knowledge, modification
or erasure of stored personal data shall be prevented (storage control);
4. The use by unauthorized persons of data processing systems from which or into which personal
data are transmitted by means of automatic equipment shall be prevented (user control);
5. It shall be ensured that persons entitled to use a data-processing system have access by means
of automatic equipment only to the personal data to which they have a right of access (access
control);
6. It shall be ensured that it is possible to check and to establish to which establishments personal
data can be communicated by means of automatic equipment (communication control);
7. It shall be ensured that it is possible to check and establish later what personal data have been
input into data-processing systems, by whom and at what time (input control);
8. It shall be ensured that personal data which are processed on behalf of third parties can be
processed only strictly in accordance with the instructions of the principal control of processing
on behalf of third parties);
9. It shall be ensured that data cannot be read, modified or erased without authorization during
their communication or during the transport of relevant storage media (transport control);  
10. It shall be ensured that the internal organization of authorities or enterprises is suited to 
the particular requirements of data protection (organization control).