Übersetzung durch den Sprachendienst des Bundesministeriums des Innern.
Translations provided by the Language Service of the Federal Ministry of the Interior.
Stand: Die Übersetzung berücksichtigt die Änderung(en) des Gesetzes durch Artikel 1 des Gesetzes vom 14.8.2009 (BGBl. I S. 2814)
Version information: The translation includes the amendment(s) to the Act by Article 1 of the Act of 14.8.2009 (Federal Law Gazette I p. 2814)

Federal Data Protection Act

Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814)
This Act serves to implement directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EC no. L 281, p. 31 ff.).

Part I
General and common provisions

Section 1
Purpose and scope

(1) The purpose of this Act is to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data.
(2) This Act shall apply to the collection, processing and use of personal data by

1. public bodies of the Federation,

2. public bodies of the Länder in so far as data protection is not governed by Land legislation and in so far as they

   a) execute federal law or,

   b) act as bodies of the judicature and are not dealing with administrative matters,

3. private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities.

(3) In so far as other legal provisions of the Federation are applicable to personal data, including their publication, such provisions shall take precedence over the provisions of this Act. This shall not affect the duty to observe the legal obligation of maintaining secrecy or professional or special official confidentiality not based on legal provisions.
(4) The provisions of this Act shall take precedence over those of the Administrative Procedures Act in so far as personal data are processed in ascertaining the facts.
(5) This Act shall not apply in so far as a controller located in another Member State of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data, except where such collection, processing or use is carried out by a branch in Germany. This Act shall apply in so far as a controller which is not located in a Member State of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data in Germany. In so far as the controller is to be named under this Act, information is also to be furnished on representatives established in Germany. Sentences 2 and 3 shall not apply in so far as data storage media are employed solely for the purposes of transit through Germany. Section 38 (1) first sentence shall remain unaffected.

Section 2
Public and private bodies

(1) “Public bodies of the Federation” means the authorities, the bodies of the judicature and other public-law institutions of the Federation, of the Federal corporations, establishments and foundations under public law as well as of their associations irrespective of their legal structure. The successor companies created from the Special Fund Deutsche Bundespost by act of law are considered public bodies as long as they have an exclusive right under the Postal Law.
(2) “Public bodies of the Länder” means the authorities, the bodies of the judicature and other public-law institutions of a Land, of a municipality, an association of municipalities or other legal persons under public law subject to Land supervision as well as of their associations irrespective of their legal structure.
(3) Private-law associations of public bodies of the Federation and the Länder performing public administration duties shall be regarded as public bodies of the Federation, irrespective of private shareholdings, if

1. they operate beyond the territory of a Land or
2. the Federation possesses the absolute majority of shares or votes.

Otherwise they shall be regarded as public bodies of the Länder.
(4) “Private bodies” means natural or legal persons, companies and other private-law associations where they are not covered by sub-sections 1 to 3 above. To the extent that a private body performs sovereign public administration duties, it shall be treated as a public body for the purposes of this Act.

Section 3
Further definitions

(1) “Personal data” means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).
(2) “Automated processing” means the collection, processing or use of personal data by means of data processing systems. 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.
(3) “Collection” means the acquisition of data on the data subject.
(4) “Processing” means the storage, modification, transfer, blocking and erasure of personal data. In particular cases, irrespective of the procedures applied:

1. “storage” means the entry, recording or preservation of personal data on a storage medium so that they can be processed or used again,
2. “modification” means the alteration of the substance of stored personal data,
3. “transfer” means the disclosure to a third party of personal data stored or obtained by means of data processing either
    a) through transmission of the data to the third party or
    b) through the third party inspecting or retrieving data held ready for inspection or retrieval,
4. “blocking” means labelling stored personal data so as to restrict their further processing or use,
5. “erasure” means the deletion of stored personal data.

(5) “Use” means any utilization of personal data other than processing.

(6) “Rendering anonymous” means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.
(6a) “Aliasing” means replacing a person’s name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.
(7) “Controller” means any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same.
(8) “Recipient” means any person or body receiving data. “Third party” means any person or body other than the controller. This shall not include the data subject or persons and bodies 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.
(9) “Special categories of personal data” means information on a person’s racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.
(10) “Mobile personal storage and processing media” means storage media

1. which are issued to the data subject,
2. on which personal data can be processed automatically beyond the storage function by the issuing body or another body and
3. which enable the data subject to influence this processing only by using the medium.

(11) “Employees” include

1. employees,
2. persons hired for the purpose of occupational training,
3. persons participating in measures to integrate them into the labour market or to clarify their ability or suitability for work (rehabilitation measures),
4. persons employed at certified workshops for persons with a disability,
5. persons employed under the Youth Volunteer Service Act,
6. persons comparable to employees due to their economic dependence, including home-based workers and those of similar status,
7. applicants for employment and those whose employment has ended,
8. civil servants, federal judges, military personnel and persons in the alternative civilian service.

Section 3a
Data reduction and data economy

Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection.

Section 4
Admissibility of data collection, processing and use

(1) The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented.
(2) Personal data shall be collected from the data subject. They may be collected without his/her participation only if

1. a legal provision prescribes or peremptorily presupposes such collection or

2.

a) the nature of the administrative duty to be performed or the business purpose necessitates collection of the data from other persons or bodies or

b) collection of the data from the data subject would necessitate disproportionate effort

and there are no indications that overriding legitimate interests of the data subject are impaired.
(3) If personal data are collected from the data subject, the controller is to inform him/her as to

1. the identity of the controller,

2. the purposes of collection, processing or use and

3. the categories of recipients only 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,

unless the data subject has already acquired such knowledge by other means. If personal data are collected from the data subject pursuant to a legal provision which makes the supply of particulars obligatory or if such supply is the prerequisite for the granting of legal benefits, the data subject shall be informed that such supply is obligatory or voluntary, as the case may be. In so far as the circumstances of the individual case dictate or at the data subject's request, he/she shall be informed of the legal provision and of the consequences of withholding particulars.

Section 4a
Consent

(1) Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.
(2) In the field of scientific research, a special circumstance pursuant to sub-Section 1 third sentence above shall also be deemed to exist where the defined purpose of research would be impaired considerably if consent were obtained in writing. In such case the information pursuant to sub-Section 1 second sentence above and the reasons from which considerable impairment of the defined purpose of research would arise shall be recorded in writing.
(3) In so far as special categories of personal data (Section 3 (9)) are collected, processed or used, the consent must further refer expressly to these data.

Section 4b
Transfer of personal data abroad and to supranational or international bodies

(1) The transfer of personal data to bodies

1. in other Member States of the European Union,

2. in other states parties to the Agreement on the European Economic Area or

3. institutions and bodies of the European Communities

shall be subject to Section 15 (1), Section 16 (1) and Sections 28 to 30a in accordance with the laws and agreements applicable to such transfer, in so far as transfer is effected in

connection with activities which fall in part or in their entirety within the scope of the law of the European Communities.
(2) Sub-Section 1 shall apply mutatis mutandis to the transfer of personal data to bodies in accordance with sub-Section 1 when effected outside of activities which fall in part or in their entirety within the scope of the law of the European Communities and to the transfer of such data to other foreign, supranational or international bodies. Transfer shall not be effected in so far as the data subject has a legitimate interest in excluding transfer, in particular if an adequate level of data protection is not guaranteed at the bodies stated in the first sentence of this sub-section. The second sentence shall not apply if transfer is necessary in order to enable a public body of the Federation to perform its duties for compelling reasons of defence or to discharge supranational or international duties in the field of crisis management or conflict prevention or for humanitarian measures.
(3) The adequacy of the afforded level of protection shall be assessed in the light of all circumstances surrounding a data transfer operation or a category of data transfer operations; particular consideration shall be given to the nature of the data, the purpose, the duration of the proposed processing operation, the country of origin, the recipient country and the legal norms, professional rules and securities measures which apply to the recipient.
(4) In the cases referred to in Section 16 (1) No. 2 above, the body transferring the data shall inform the data subject of the transfer of his/her data. This shall not apply if it can be assumed that the data subject will acquire knowledge of such transfer in another manner or if such information would jeopardize public safety or otherwise be detrimental to the Federation or a Land.
(5) Responsibility for the admissibility of the transfer shall rest with the body transferring the data.
(6) The body to which the data are transferred shall be informed of the purpose for which the data are transferred.

Section 4c
Exceptions

(1) In connection with activities which fall in part or in their entirety within the scope of the law of the European Communities, the transfer of personal data to bodies other than those stated in Section 4b (1) above shall be admissible even if such bodies do not guarantee an adequate level of data protection, in so far as

1. the data subject has given his/her consent,

2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request,

3. 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,

4. the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims,

5. the transfer is necessary in order to protect the vital interests of the data subject,

6. the transfer is made from a register which is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the statutory conditions are fulfilled in the particular case.

It shall be pointed out to the recipient body that the transferred data may be processed or used only for the purpose for which they have been transferred.

(2) Without prejudice to the first sentence of Section 1, the competent supervisory authority may authorize individual transfers or certain categories of transfers of personal data to bodies other than those stated in Section 4b (1) above, if the controller adduces adequate safeguards with respect to the protection of privacy and exercise of the corresponding rights; such safeguards may in particular result from contractual clauses or binding corporate regulations. In the case of postal and telecommunications companies, competence lies with the Federal Commissioner for Data Protection and Freedom of Information. In so far as transfer is to be effected by public bodies, the latter shall carry out the examination in accordance with the first sentence of Section 1 above.
(3) The Länder shall notify the Federation of the decisions made in accordance with sentence 1 of Section 2 above.

Section 4d
Obligatory registration

(1) Prior to putting automated processing procedures into operation, private controllers shall register such procedures with the competent supervisory authorities, while federal controllers and controllers of postal and telecommunications companies shall register such procedures with the Federal Commissioner for Data Protection and Freedom of Information in accordance with Section 4e.
(2) Obligatory registration shall not apply if the controller has appointed a data protection official.
(3) Obligatory registration shall further not apply if the controller collects, processes or uses personal data for its own purposes, provided that, as a rule, no more than nine employees are permanently employed in collecting, processing or using personal data and either consent has been obtained from the data subject or the collection, processing or use is needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject.
(4) Sub-sections 2 and 3 above shall not apply in cases of automated processing in which the controller concerned stores personal data in the course of business

1. for the purpose of transfer,
2. for the purpose of anonymized transfer, or
3. for the purpose of market or opinion research.

(5) In so far as automated processing operations involve risks for the rights and liberties of the data subject, they are subject to examination prior to the beginning of processing (prior checking). Prior checking is to be carried out in particular when

1. special categories of personal data (Section 3 (9)) are to be processed or
2. the processing of personal data is intended to appraise the data subject's personality, including his abilities, performance or conduct,

unless a statutory obligation applies, the data subject's consent has been obtained, or the collection, processing or use is needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject.
(6) Prior checking is the responsibility of the data protection official. The latter shall carry out prior checking after receiving the list in accordance with Section 4g (2) first sentence. In cases of doubt, he is to refer to the supervisory authority or, in the case of postal and telecommunications companies, to the Federal Commissioner for Data Protection and Freedom of Information.

Section 4e
Contents of the obligatory registration

In so far as automated processing procedures are subject to obligatory registration, the following information is to be furnished:

1. Name or title of the controller,

2. owners, managing boards, managing directors or other lawfully or constitutionally appointed managers and the persons placed in charge of data processing,

3. address of the controller,

4. purposes of collecting, processing or using data,

5. a description of the groups of data subjects and the appurtenant data or categories of data,

6. recipients or categories of recipients to whom the data may be transferred,

7. standard periods for the erasure of data,

8. any planned data transfer in third states,

9. a general description enabling preliminary assessment as to whether the measures in accordance with Section 9 to guarantee the safety of processing are adequate.

Section 4d (1) and (4) shall apply mutatis mutandis to the amendment of information furnished in accordance with sentence 1 above and to the time of commencement and termination of the activity subject to obligatory registration.

Section 4f
Data protection official

(1) Public and private bodies which process personal data automatically shall appoint in writing a data protection official. Private bodies are obliged to appoint such an officer within one month of commencing their activities. The same shall apply where personal data are processed by other means and at least 20 persons are permanently employed for this purpose. The first and second sentences above shall not apply to private bodies which generally deploy a maximum of nine employees to carry out the automatic processing of personal data on an ongoing basis. In so far as the structure of a public body requires, the appointment of one data protection official for several areas shall be sufficient. In so far as private bodies carry out automated processing operations which are subject to prior checking or process personal data in the course of business for the purposes of transfer, anonymized transfer, or market or opinion research, they are to appoint a data protection official irrespective of the number of persons deployed to carry out automatic processing.
(2) Only persons who possess the specialized knowledge and demonstrate the reliability necessary for the performance of the duties concerned may be appointed data protection official. The required level of specialized knowledge is determined in particular according to the scope of data processing carried out by the controller concerned and the protection requirements of the personal data collected or used by the controller concerned. A person from outside the body concerned may also be appointed data protection official; monitoring shall also extend to personal data which are subject to professional or official secrecy, in particular tax secrecy pursuant to Section 30 of the Fiscal Code.
(3) The data protection official shall be directly subordinate to the head of the public or private body. He or she shall be free to use his/her specialized knowledge in the area of data protection. He/she shall suffer no disadvantage through the performance of his/her duties. The appointment of a data protection official may be revoked by applying Section 626 of the Civil Code mutatis mutandis or, in the case of private bodies, at the request of the supervisory authority. If a data protection official is to be appointed under sub-Section 1, then

this appointment shall not be subject to termination, unless there is reason for the controller to terminate the appointment for just cause without complying with a notice period. After the data protection official has been removed from office, he or she cannot be terminated for a year following the end of the appointment unless the responsible body has just cause for termination without complying with a notice period. The controller shall enable the data protection official to take part in advanced training measures and shall assume the expense of such measures, in order for the data protection official to maintain the expertise needed to perform his/her tasks.
(4) The data protection official shall be bound to maintain secrecy on the identity of the data subject and on circumstances permitting conclusions to be drawn about the data subject, unless he/she is released from this obligation by the data subject.
(4a) In so far as the data protection official obtains knowledge of data in the course of his or her activities in connection with which a right of refusal to give evidence applies on professional grounds to the head of the public or private body or a person employed at such a body, this right shall also apply to the data protection official and his/her assistants. The person to whom the right of refusal to give evidence applies on professional grounds shall decide whether to exercise this right, except where it will not be possible to effect such a decision in the foreseeable future. To the extent to which the data protection official's right of refusal to give evidence applies, the data protection official's files and other documentation shall be subject to a prohibition of seizure.
(5) The public and private bodies shall support the data protection official in the performance of his/her duties and in particular, to the extent needed for such performance, make available assistants as well as premises, furnishings, equipment and other resources. Data subjects may approach the data protection official at any time.

Section 4g
Duties of the data protection official

(1) The data protection official shall work to ensure compliance with this Act and other data protection provisions. For this purpose, the data protection official may consult the competent authority responsible for data protection control with regard to the controller concerned. In particular, he shall

1. monitor the proper use of data processing programs with the aid of which personal data are to be processed; for this purpose he/she shall be informed in good time of projects for automatic processing of personal data,

2. take suitable steps to familiarize the persons employed in the processing of personal data with the provisions of this Act and other provisions concerning data protection, and with the various special requirements of data protection.

The data protection official may avail him- or herself of the advisory services pursuant to Section 38 (1), sentence 2.
(2) The controller shall provide the data protection official with an overview of the information stipulated in Section 4e first sentence and a list of persons entitled to access. The data protection official shall, on request, make the information pursuant to Section 4e first sentence Nos. 1 to 8 available to anyone in an appropriate manner.
(2a) Where no obligation to appoint a data protection official applies at a private body, the head of the private body is to ensure due discharge of the duties pursuant to sub-sections 1 and 2.
(3) Sentence 2 of Section 2 shall not apply to the authorities stated in sentence 4 of Section 6 (2). Sentence 2 of Section 1 shall apply on condition that the authority's data protection official contacts the head of the authority; any disagreements between the authority's data protection official and the head of the authority shall be settled by the supreme federal authority.

Section 5
Confidentiality

Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality). On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.

Section 6
Rights of the data subject

(1) The data subject's right of access (Sections 19, 34) and to correction, erasure or blocking (Sections 20, 35) may not be excluded or restricted by a legal transaction.
(2) If the data of the data subject are stored by means of automated procedures such that several bodies are entitled to store and if the data subject is unable to ascertain which body has stored the data, he may approach any of these bodies. Such body is obliged to forward the request of the data subject to the body which has stored the data. The data subject shall be informed of the forwarding of the request and of the identity of the body concerned. The bodies listed in Section 19 (3) of this Act, public prosecution and police authorities as well as public finance authorities may, in so far as they store personal data in performing their legal duties within the area of application of the Fiscal Code for monitoring and control purposes, inform the Federal Commissioner for Data Protection and Freedom of Information instead of the data subject. In such case the further procedure shall be as described in Section 19 (6) of this Act.
(3) Personal data concerning the data subject's exercise of a right based on this or another law on data protection may be used only to fulfil obligations of the responsible body arising from the exercise of this right.

Section 6a
Automated individual decision

(1) Decisions which have legal consequences for or substantially impair the interests of the data subject must not be based exclusively on the automated processing of personal data which serve to evaluate individual personal characteristics. In particular, a decision not made by a natural person based on the evaluation of content shall constitute a decision based exclusively on automated processing.
(2) This shall not apply if

1. the decision is made in connection with the conclusion or fulfilment of a contract or any other legal relationship and the data subject's request has been met or
2. if there are appropriate measures to protect the legitimate interests of the data subject and the controller informs the data subject that a decision as referred to in sub-Section 1 has been made and, upon request, explains the main reasons for this decision.

(3) The data subject's right of access in accordance with Sections 19 and 34 shall also extend to the logic of the processing of his/her personal data.

Section 6b
Monitoring of publicly accessible areas with optic-electronic devices

(1) Monitoring publicly accessible areas with optic-electronic devices (video surveillance) is allowable only in so far as it is necessary

1. to fulfil public tasks,
2. to exercise the right to determine who shall be allowed or denied access or
3. to pursue rightful interests for precisely defined purposes

and if there are no indications that the data subjects' legitimate interests prevail.

(2) The fact that the area is being monitored and the controller's identity shall be made discernible by appropriate means.
(3) Data that have been collected under sub-Section 1 above may be processed or used if this is necessary for the pursued purpose and if there are no indications that the data subjects' legitimate interests prevail. They may only be processed or used for another purpose if this is necessary to avert dangers to state security or public safety or to prosecute crimes.
(4) Where data collected through video-surveillance are attributed to an identified person, this person shall be informed about such processing or use in conformity with Sections 19a and 33.
(5) The data shall be deleted without delay, if they are no longer needed for the pursued purpose or if the data subject's legitimate interests stand in the way of any further storage.

Section 6c
Mobile storage and processing media for personal data

(1) A body which issues a mobile storage and processing medium for personal data or which applies a procedure for the automated processing of personal data which runs in part or in its entirety on such a medium to the medium or modifies or makes such data available must inform the data subject

1. of its identity and address,
2. of the medium's mode of functioning in generally comprehensible terms, including the type of personal data to be processed,
3. how he can exercise his rights in accordance with Sections 19, 20, 34 and 35, and
4. of the measures to be undertaken in the event of loss or destruction of the medium,

in so far as the data subject has not already acquired such knowledge.

(2) The body which is subject to the obligations stipulated in sub-Section 1 shall ensure that devices or facilities which are necessary in order to enable the data subject to assert his right of access are available in adequate numbers for use free of charge.
(3) Communications procedures which initiate data processing on the medium must be clearly apparent to the data subject.

Section 7
Compensation

Where a controller causes harm to the data subject through the collection, processing or use of his/her personal data that is inadmissible or incorrect under the provisions of this Act or other data protection provisions, such controller or its supporting organization shall be obliged to compensate the data subject for the harm thus caused. This obligation to provide compensation shall not apply if the controller has exercised due care in accordance with the circumstances of the case concerned.

Section 8
Compensation in case of automated data processing by public bodies

(1) Where a public body causes harm to the data subject through the automated collection, processing or use of his/her personal data that is inadmissible or incorrect under the provisions of this Act or other data protection provisions, such body's supporting organization shall be obliged to compensate the data subject for the harm thus caused, irrespective of any fault.
(2) In grave cases of violation of privacy, the data subject shall receive adequate pecuniary compensation for the immaterial harm caused.

(3) The claims under sub-sections 1 and 2 above shall be limited to a total amount of € 130,000. Where, due to the same occurrence, compensation has to be paid to several persons and exceeds the maximum amount of € 130,000, the compensation paid to each of them shall be reduced in proportion to the maximum amount.
(4) If, in the case of automated processing, several bodies are entitled to store the data and the injured person is unable to ascertain the controller of the filing system, each body shall be liable.
(5) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.
(6) The limitation provisions stipulated for tortious acts in the Civil Code shall apply mutatis mutandis with regard to statutory limitation.

Section 9
Technical and organizational measures

Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection.

Section 9a
Data protection audit

In order to improve data protection and data security, suppliers of data processing systems and programs and bodies conducting data processing may have their data protection strategies and their technical facilities examined and evaluated by independent and approved appraisers, and may publish the result of the audit. The detailed requirements pertaining to examination and evaluation, the procedure and selection and approval of the appraisers shall be stipulated in a separate act.

Section 10
Establishment of automated retrieval procedures

(1) An automated procedure for the retrieval of personal data may be established in so far as such procedure is appropriate, having due regard to the legitimate interests of the data subjects and to the duties or business purposes of the bodies involved. The provisions on the admissibility of retrieval in a particular case shall remain unaffected.
(2) The bodies involved shall ensure that the admissibility of the retrieval procedure can be monitored. For such purpose they shall specify in writing:

1. the reason for and purpose of the retrieval procedure,
2. third parties to whom transfer is effected,
3. the type of data to be transferred,
4. the technical and organizational measures required under Section 9 of this Act.

In the public sector the supervisory authorities may lay down such specifications.
(3) In cases where the bodies mentioned in Section 12 (1) of this Act are involved, the Federal Commissioner for Data Protection and Freedom of Information shall be notified of the establishment of retrieval procedures and of the specifications made under sub-Section 2 above. The establishment of retrieval procedures in which the bodies mentioned in Sections 6 (2) and 19 (3) of this Act are involved shall be admissible only if the federal or Land ministries responsible for the controller of the filing system and for the retrieving body or their representatives have given their consent.
(4) Responsibility for the admissibility of retrieval in a particular case shall rest with the third party to whom transfer is effected. The controller of the filing system shall examine the admissibility of retrieval only if there is cause for such examination. The controller of the filing

system shall ensure that the transfer of personal data can be ascertained and checked at least by means of suitable sampling procedures. If all personal data are retrieved or transferred (batch processing), it shall be sufficient to ensure that the admissibility of the retrieval or transfer of all data can be ascertained and checked.
(5) Sub-sections 1 to 4 above shall not apply to the retrieval of generally accessible data. Generally accessible data are data which anyone can use, be it with or without prior registration, permission or the payment of a fee.

Section 11
Commissioned collection, processing or use of personal data

(1) Where other bodies are commissioned to collect, process or use personal data, responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal. The rights referred to in Sections 6, 7 and 8 of this Act shall be asserted vis-à-vis the principal.
(2) The agent shall be carefully selected, with particular regard for the suitability of the technical and organizational measures taken by him/her. The commission shall be given in writing, specifying the collection, processing and use of the data, the technical and organizational measures and any subcommissions. The commission shall be given in writing and shall specify in particular:

1. the subject and the duration of the commission,
2. the extent, type and purpose of the planned collection, processing or use of data; the type of data and group of persons affected,
3. technical and organizational measures to be taken under Section 9,
4. the correction, erasure and blocking of data,
5. the agent's obligation under sub-Section 4, in particular controls to be undertaken,
6. any right to issue subcontracts,
7. the principal's rights of control and the agent's corresponding obligations to tolerate and cooperate,
8. violations by the agent or persons employed by him/her of provisions to protect personal data or of terms specified in the commission which must be reported,
9. the extent of the principal's authority to issue instructions to the agent,
10. the return of data storage media and the erasure of data stored by the agent after the commission has been completed.

In the case of public bodies, the commission may be given by the supervisory authority. The principal shall verify compliance with the technical and organizational measures undertaken by the agent before data processing begins and regularly thereafter. The result shall be documented.
(3) The agent may collect, process or use the data only as instructed by the principal. If the agent thinks that an instruction of the principal infringes this Act or other data protection provisions, he/she shall point this out to the principal without delay.
(4) For the agent the only applicable provisions other than those of Sections 5, 9, 43 (1), Nos. 2, 10 and 11, (2) Nos. 1 to 3 and (3) and Section 44 of this Act shall be the provisions on data protection control or supervision, namely for

1.
   a) public bodies,

b) private bodies where the public sector possesses the majority of shares or votes and where the principal is a public body,

Sections 18, 24 to 26 of this Act or the relevant data protection laws of the Länder,

2. other private bodies in so far as they are commissioned to collect, process or use personal data in the course of business as service enterprises, Sections 4 f, 4 g and 38 of this Act.

(5) Sub-sections 1 to 4 shall apply mutatis mutandis if other bodies are commissioned to carry out the inspection or maintenance of automated procedures or data processing systems, in the course of which the possibility of personal data being accessed cannot be excluded.

Part II
Data processing by public bodies

Chapter I
Legal basis for data processing

Section 12
Scope

(1) The provisions of this Part shall apply to public bodies of the Federation in so far as they do not participate in competition as public-law enterprises.
(2) Where data protection is not governed by Land legislation, Sections 12 to 16, 19 and 20 of this Act shall also apply to public bodies of the Länder in so far as they

1. execute federal law and do not participate in competition as public-law enterprises or

2. act as bodies of the judicature and are not dealing with administrative matters.

(3) Section 23 (4) of this Act shall apply mutatis mutandis to Land commissioners for data protection.
(4) If personal data are collected, processed or used for the purpose of past, present or future employment contracts, Section 28 (2) No. 2 and Sections 32 to 35 of this Act shall apply instead of Sections 13 to 16 and 19 to 20.

Section 13
Collection of data

(1) The collection of personal data shall be admissible if knowledge of them is needed to perform the duties of the bodies collecting them.
(1a) Where personal data are collected from a private body and not from the data subject, such body shall be informed of the legal provision requiring the supply of particulars or that such supply is voluntary, as the case may be.
(2) The collection of special types of personal data (Section 3 (9)) is permissible only in so far as

1. such collection is stipulated in a legal provision or essential on account of an important public interest,

2. the data subject has consented pursuant to Section 4a (3) of this Act,

3. such collection is necessary in order to protect vital interests of the data subject or of a third party, in so far as the data subject is unable to give his/her consent for physical or legal reasons,

4. such collection concerns data which the data subject has evidently made public,

5. such collection is necessary in order to avert a substantial threat to public safety,

6. such collection is necessary in order to avert substantial detriment to the common weal or to protect substantial interests of the common weal,

7. such collection is necessary for the purposes of preventive medicine, medical diagnosis, health care or the administration of health services and the processing of these data is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy,

8. such collection is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project substantially outweighs the data subject's interest in excluding collection and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort, or

9. such collection is necessary in order to enable a public body of the Federation to perform its duties for compelling reasons of defence or to discharge supranational or international duties in the field of crisis management or conflict prevention or for humanitarian measures.

Section 14
Storage, modification and use of data

(1) The storage, modification or use of personal data shall be admissible where it is necessary for the performance of the duties of the controller of the filing system and if it serves the purposes for which the data were collected. If there has been no preceding collection, the data may be modified or used only for the purposes for which they were stored.
(2) Storage, modification or use for other purposes shall be admissible only if

1. a legal provision prescribes or peremptorily presupposes this,

2. the data subject has consented,

3. it is evident that this is in the interest of the data subject and there is no reason to assume that he/she would withhold consent if he/she knew of such other purpose,

4. particulars supplied by the data subject have to be checked because there are actual indications that they are incorrect,

5. the data are generally accessible or the controller would be permitted to publish them, unless the data subject clearly has an overriding legitimate interest in excluding the change of purpose,

6. this is necessary in order to avert substantial detriment to the common weal or a threat to public security, or to protect substantial interests of the common weal,

7. this is necessary to prosecute criminal or administrative offences, to implement sentences or measures as defined in Section 11 (1), No. 8 of the Penal Code or reformatory or disciplinary measures as defined in the Youth Courts Act, or to execute decisions imposing administrative fines,

8. this is necessary to avert a grave infringement of another person’s rights or

9. this is necessary in order to conduct scientific research, scientific interest in conduct of the research project substantially outweighs the interest of the data subject in excluding the change of purpose, and the research purpose cannot be attained by other means or can be attained thus only with disproportionate effort.

(3) Processing or use for other purposes shall not be deemed to occur if this serves the exercise of powers of supervision or control, the execution of auditing or the conduct of organizational studies for the controller of the filing system. This shall also apply to processing or use for training and examination purposes by the controller, unless the data subject has overriding legitimate interests.
(4) Personal data stored exclusively for the purpose of monitoring data protection, safeguarding data or ensuring proper operation of a data processing system may be used exclusively for such purposes.
(5) The storage, modification or use of special types of personal data (Section 3 (9)) for other purposes shall be permissible only if

1. the requirements which would permit collection in accordance with Section 13 (2), Nos. 1 to 6 or No. 9 are met or

2. this is necessary for the conduct of scientific research, scientific interest in conduct of the research project substantially outweighs the interest of the data subject in excluding the change of purpose, and the research purpose cannot be attained by other means or can be attained thus only with disproportionate effort.

In weighing up the circumstances in accordance with sentence 1, No. 2, the scientific interest in the research project is to receive special consideration in the context of the public interest.
(6) The storage, modification or use of special types of personal data (Section 3 (9)) for the purposes stated in Section 13 (2), No. 7 shall be subject to the obligations to maintain secrecy which apply to the persons stated in Section 13 (2), No. 7.

Section 15
Transfer of data to public bodies

(1) The transfer of personal data to public bodies shall be admissible if

1. this is necessary for the performance of duties of the transferring body or the third party to whom the data are transferred and

2. the requirements of Section 14 of this Act are met.

(2) Responsibility for the admissibility of transfer shall rest with the transferring body. If the data are transferred at the request of the third party to whom the data are transferred, the latter shall bear responsibility. In such case the transferring body shall merely examine whether the request for transfer lies within the remit of the third party to whom the data are transferred, unless there is special reason to examine the admissibility of transfer. Section 10 (4) of this Act shall remain unaffected.
(3) The third party to whom the data are transferred may process or use the transferred data for the purpose for which they were transferred. Processing or use for other purposes shall be admissible only if the requirements of Section 14 (2) of this Act are met.
(4) Sub-sections 1 to 3 above shall apply mutatis mutandis to the transfer of personal data to bodies of public-law religious societies, provided it is ensured that the latter take adequate data protection measures.
(5) Where personal data that may be transferred under sub-Section 1 above are linked to other personal data of the data subject or a third party in such a way that separation is not possible or is possible only with unreasonable effort, transfer of the latter data shall also be admissible, unless the data subject or a third party clearly has an overriding justified interest in keeping them secret; use of these data shall be inadmissible.
(6) Sub-Section 5 above shall apply mutatis mutandis if personal data are transmitted within a public body.

Section 16
Transfer of data to private bodies

(1) The transfer of personal data to private bodies shall be admissible if

1. this is necessary for the performance of the duties of the transferring body and the requirements of Section 14 of this Act are met or

2. the third party to whom the data are transferred credibly proves a justified interest in knowledge of the data to be transferred and the data subject does not have a legitimate interest in excluding their transfer. By way of derogation from sentence 1, No. 2, the transfer of special types of personal data (Section 3 (9)) is permissible only if the requirements which would permit use in accordance with Section 14 (5) and (9) are met, or in so far as this is necessary in order to assert, exercise or defend legal claims.

(2) Responsibility for the admissibility of transfer shall rest with the transferring body.
(3) In cases of transfer under sub-Section 1, No. 2 above, the transferring body shall inform the data subject of the transfer of his data. This shall not apply if it can be assumed that he will acquire knowledge of such transfer in another manner or if such information would jeopardize public safety or otherwise be detrimental to the Federation or a Land.
(4) The third party to whom the data are transferred may process or use the transferred data only for the purpose for which they were transferred to him. The transferring body shall point this out to him. Processing or use for other purposes shall be admissible if transfer under sub-Section 1 above would be admissible and the transferring body has consented.

Section 17
Transfer of data to bodies outside the area of application of this Act

deleted

Section 18
Implementation of data protection in the federal administration

(1) The supreme federal authorities, the President of the Federal Railway Property as well as the federal corporations, establishments and foundations under public law subject to only legal supervision by the Federal Government or a supreme federal authority shall ensure that this Act and other legal provisions concerning data protection are implemented in their respective spheres of activity. The same shall apply to the managing boards of the successor companies created from the Special Fund Deutsche Bundespost by act of law as long as they have an exclusive right under the Postal Law.
(2) Public bodies shall keep a register of the data processing systems used. In respect of their automated processing operations, they shall record the information in accordance with Section 4e and the legal basis for processing in writing. This requirement can be waived in the case of automated processing operations for administrative purposes which involve no restrictions of the data subject's right of access in accordance with Section 19 (3) or (4). The specifications may be combined for automated processing operations which are conducted several times in the same manner or a similar manner.

Chapter II
Rights of the data subject

Section 19
Provision of information to the data subject

(1) The data subject shall, at his request, be provided with information on

1. stored data concerning him, including any reference in them to their origin,

2. the recipients or categories of recipients to whom the data are transmitted, and

3. the purpose of storage.

The request should specify the type of personal data on which information is to be provided. If the personal data are stored neither by automated procedures nor in non-automated filing systems, information shall be provided only in so far as the data subject supplies particulars making it possible to locate the data and the effort needed to provide the information is not

out of proportion to the interest in such information expressed by the data subject. The controller shall exercise due discretion in determining the procedure for providing such information and, in particular, the form in which it is provided.
(2) Sub-Section 1 above shall not apply to personal data which are stored merely because they may not be erased due to legal, statutory or contractual provisions on their retention or exclusively serve purposes of data security or data protection control and the provision of information would require disproportionate effort.
(3) If the provision of information relates to the transfer of personal data to authorities for the protection of the constitution, to the Federal Intelligence Service, the Federal Armed Forces Counterintelligence Office and, where the security of the Federation is concerned, other authorities of the Federal Ministry of Defence, it shall be admissible only with the consent of such bodies.
(4) Information shall not be provided if

1. this would be prejudicial to the proper performance of the duties of the controller,

2. this would impair public safety or order or otherwise be detrimental to the Federation or a Land or

3. the data or the fact that they are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party

and for this reason the interest of the data subject in the provision of information must be subordinated.
(5) Reasons need not be stated for the refusal to provide information if the statement of the actual and legal reasons on which the decision is based would jeopardize the purpose pursued by refusing to provide information. In such case it shall be pointed out to the data subject that he/she may appeal to the Federal Commissioner for Data Protection and Freedom of Information.
(6) If no information is provided to the data subject, it shall at his/her request be supplied to the Federal Commissioner for Data Protection and Freedom of Information unless the relevant supreme federal authority determines in a particular case that this would jeopardize the security of the Federation or a Land. The transfer from the Federal Commissioner to the data subject must not allow any conclusions to be drawn as to the knowledge at the disposal of the controller, unless the latter consents to more extensive information being provided.
(7) Information shall be provided free of charge.

Section 19a
Notification

(1) If data are collected without the data subject's knowledge, he/she is to be informed of storage, of the controller's identity and of the purposes of collection, processing or use. The data subject is also to be notified of the recipients or categories of recipients of data, except where he/she must expect transfer to such recipients. When transfer is envisaged, notification is to be provided at the time of the first transfer at the latest.
(2) Notification shall not be required if

1. the data subject has received knowledge by other means of the storage or transfer of the data,

2. notification of the data subject would require disproportionate effort or

3. the law expressly provides for storage or transfer of the personal data.

The controller shall stipulate in writing under what conditions notification shall not be provided in accordance with Nos. 2 or 3 above.
(3) Section 19 (2) to (4) shall apply mutatis mutandis.

Section 20
Correction, erasure and blocking of data; right of objection

(1) Incorrect personal data shall be corrected. If it is established that personal data which have neither been processed by automated procedures nor stored in automated filing systems are incorrect, or if their accuracy is contested by the data subject, this is to be recorded in an appropriate manner.
(2) Personal data which are processed by automated procedures or stored in non-automated filing systems are to be erased if

1. their storage is inadmissible or
2. knowledge of them is no longer required by the controller of the filing system for the performance of his duties.

(3) Instead of erasure, personal data shall be blocked in so far as

1. retention periods prescribed by law, statutes or contracts rule out any erasure,
2. there is reason to assume that erasure would impair legitimate interests of the data subject or
3. erasure is not possible or is only possible with disproportionate effort due to the specific type of storage.

(4) Personal data which are processed by automated procedures or stored in non-automated filing systems shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect.
(5) Personal data must not be collected, processed or used for automated processing or processing in non-automated filing systems if the data subject files an objection with the controller and an examination reveals that the data subject's legitimate interest outweighs the controller's interest in such collection, processing or use, on account of the data subject's personal situation. Sentence 1 shall apply only when an obligation to carry out collection, processing or use is established by a legal provision.
(6) Personal data which are neither processed by automatic procedures nor stored in a non-automated filing system are to be blocked if, in the individual case concerned, the authority establishes that legitimate interests of the data subject would be impaired without such blockage and the data are no longer required in order for the authority to be able to discharge its duties.
(7) Blocked data may be transferred or used without the consent of the data subject only if

1. this is indispensable for scientific purposes, for use as evidence or for other reasons in the overriding interests of the controller of the data or a third party and
2. transfer or use of the data for this purpose would be admissible if they were not blocked.

(8) The correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage shall be notified to the bodies to which these data are transmitted for storage within the framework of regular data transfer, provided that this does not require disproportionate effort and does not conflict with any legitimate interests of the data subject.
(9) Section 2 (1) to (6), (8) and (9) of the Federal Archives Act shall apply.

Section 21
Appeals to the Federal Commissioner for Data Protection and Freedom of Information

Anyone may appeal to the Federal Commissioner for Data Protection and Freedom of Information if he or she believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies of the Federation.

This shall apply to the collection, processing or use of personal data by courts of the Federation only in so far as they deal with administrative matters.

Chapter III
Federal Commissioner for Data Protection and Freedom of Information

Section 22
Election of the Federal Commissioner for Data Protection and Freedom of Information

(1) On a proposal from the Federal Government the Bundestag shall elect the Federal Commissioner for Data Protection and Freedom of Information with over half of the statutory number of its members. The Federal Commissioner must be at least 35 years old at the time of his election. The person elected shall be appointed by the Federal President.
(2) The Federal Commissioner 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 them from harm and to defend the Basic Law and the laws of the Federation, 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 Commissioner shall be five years. It may be renewed once.
(4) The Federal Commissioner shall, as directed by this Act, have public-law official status with respect to the Federation. He or she shall be independent in the performance of his/her duties and subject to the law only. He or she shall be subject to the legal supervision of the Federal Government.
(5) The Federal Commissioner shall be established with the Federal Minister of the Interior. He or she shall be subject to the hierarchical supervision of the Federal Minister of the Interior. The Federal Commissioner shall be provided with the personnel and material resources necessary for the performance of his/her duties; these resources shall be shown in a separate chapter of the budget of the Federal Minister of the Interior. The posts shall be filled in agreement with the Federal Commissioner. If they do not agree to the envisaged measure, staff members may be transferred, delegated or relocated only in agreement with the Federal Commissioner.
(6) If the Federal Commissioner is temporarily prevented from performing his/her duties, the Federal Minister of the Interior may appoint a substitute to perform such duties. The Federal Commissioner shall be consulted on such appointment.

Section 23
Legal status of the Federal Commissioner for Data Protection and Freedom of Information

(1) The mandate of the Federal Commissioner for Data Protection and Freedom of Information shall commence on delivery of the certificate of appointment. It shall end

1. on expiry of his/her term of office,
2. on his/her dismissal.

The Federal President shall dismiss the Federal Commissioner at the latter’s request or on a proposal by the Federal Government when there are grounds which, in the case of an established judge, justify dismissal from service. In the event of termination of office, the Federal Commissioner 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 Commissioner shall be obliged to continue his/her work until a successor has been appointed.
(2) The Federal Commissioner shall not hold any other paid office or pursue any gainful activity or occupation in addition to his/her official duties and shall not belong to the management, supervisory board or board of directors of a profit-making enterprise nor to a

government or a legislative body of the Federation or a Land. He or she may not deliver extra-judicial opinions in exchange for payment.
(3) The Federal Commissioner shall inform the Federal Ministry of the Interior of any gifts received in the performance of his/her duties. The Federal Ministry of the Interior shall decide how such gifts shall be used.
(4) The Federal Commissioner shall be entitled to refuse to give testimony as a witness on persons who have entrusted information to him/her in his/her capacity as Federal Commissioner and on such information itself. This shall also apply to the staff of the Federal Commissioner, on condition that the Federal Commissioner decides on the exercise of this right. Within the scope of the Federal Commissioner's right to refuse to give testimony as a witness, he/she may not be required to submit or surrender files or other documents.
(5) The Federal Commissioner shall be obliged, even after termination of his/her service, to maintain secrecy concerning information of which he/she has knowledge by reason of his/her 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 Commissioner 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 Ministry of the Interior. This provision shall not, however, affect his/her duty by law to report criminal offences and to take action to uphold the free democratic fundamental order whenever it is jeopardized. Sections 93, 97, 105 (1), Section 111 (5) in conjunction with Section 105 (1) and Section 116 (1) of the Fiscal Code shall not apply to the Federal Commissioner for Data Protection and his/her staff in so far as the fiscal authorities require such knowledge in order to conduct legal proceedings due to a tax offence and a related tax procedure, the prosecution of which is necessary on account of a compelling public interest, or in so far as the person obliged to provide information or persons acting on his behalf have intentionally provided false information. If the Federal Commissioner establishes a violation of data protection provisions, he/she shall be authorized to file charges and to inform the data subject accordingly.
(6) Consent to give testimony as a witness shall be refused only when such testimony would be to the detriment of the Federation or a Land or seriously jeopardize or impede the performance of public duties. Consent to deliver an opinion may be refused where it would be against the interest of the service. Section 28 of the Act on the Federal Constitutional Court shall remain unaffected.
(7) From the beginning of the calendar month in which he/she commences his/her duties until the end of the calendar month in which he/she terminates his/her duties or, in the event of sub-Section 1 sixth sentence above being applied, until the end of the month in which his/her activities cease, the Federal Commissioner shall receive the remuneration of a grade B 9 federal official. The Federal Act on Travel Expenses and the Federal Act on Removal Expenses shall apply mutatis mutandis. In all other respects, Section 12 (6) and Sections 13 to 20 and 21a (5) of the Act on Federal Ministers shall apply, except that the period of office of four years provided in Section 15 (1) of the Act on Federal Ministers shall be replaced by a period of office of five years and pay grade B 11 as stipulated in Section 21a (5) of the Act on Federal Ministers shall be replaced by pay grade B 9. Notwithstanding the third sentence above in conjunction with Sections 15 to 17 and 21a (5) of the Act on Federal Ministers, the pension of the Federal Commissioner shall be calculated, taking account of the pensionable period of service, on the basis of the Civil Servants Pensions Act if this is more favourable and if, immediately before his/her election, the Federal Commissioner held as a civil servant or judge at least the last position customarily required before reaching the B 9 pay grade.
(8) Sentences 5 to 7 of sub-Section 5 shall apply mutatis mutandis to the public bodies which are responsible for monitoring compliance with the provisions on data protection in the individual Länder.

Section 24
Monitoring by the Federal Commissioner for Data Protection and Freedom of Information

(1) The Federal Commissioner for Data Protection and Freedom of Information shall monitor compliance with the provisions of this Act and other data protection provisions by public bodies of the Federation.
(2) Monitoring by the Federal Commissioner shall also extend to

1. personal data obtained by public bodies of the Federation on the contents of and the specific circumstances relating to correspondence, postal communications and telecommunications and

2. personal data subject to professional or special official secrecy, especially tax secrecy under Section 30 of the Tax Code.

The fundamental right to privacy of correspondence, posts and telecommunications as enshrined in Article 10 of the Basic Law is in so far curtailed. Personal data subject to monitoring by the commission set up under Section 15 of the Act on Article 10 shall not be subject to monitoring by the Federal Commissioner unless the commission requests the Federal Commissioner to monitor compliance with data protection provisions in connection with specific procedures or in specific areas and to report thereon exclusively to it. Personal data in files on the security check shall not be subject to monitoring by the Federal Commissioner if the data subject files a complaint with the Federal Commissioner objecting to monitoring of the data relating to his/her person in the individual case concerned.
(3) The activities of judges at federal courts which directly serve the purposes of adjudication shall be exempted from monitoring.
(4) Public bodies of the Federation shall be obliged to support the Federal Commissioner and his assistants in the performance of their duties. In particular they shall be granted

1. information in reply to their questions as well as the opportunity to inspect all documents, especially stored data and data processing programs, connected with the monitoring referred to in sub-Section 1 above,

2. access to all official premises at any time.

The authorities referred to in Sections 6 (2) and 19 (3) of this Act shall afford support exclusively to the Federal Commissioner himself and the assistants appointed by him in writing. The second sentence above shall not apply to such authorities where the supreme federal authority establishes in a particular case that such information or inspection would jeopardize the security of the Federation or a Land.
(5) The Federal Commissioner shall inform the public body of the results of his monitoring. He or she may combine them with proposals for improving data protection, especially for rectifying irregularities discovered in the processing or use of personal data. Section 25 of this Act shall remain unaffected.
(6) Sub-Section 2 above shall apply mutatis mutandis to public bodies responsible for monitoring compliance with data protection provisions in the Länder.

Section 25
Complaints lodged by the Federal Commissioner for Data Protection and Freedom of Information

(1) Should the Federal Commissioner for Data Protection and Freedom of Information discover infringements of this Act or of other data protection provisions or other irregularities in the processing or use of personal data, he/she shall lodge a complaint

1. in the case of the federal administration, with the competent supreme federal authority,

2. in the case of the Federal Railway Property, with the President,

3. in the case of the successor companies created from the Special Fund Deutsche Bundespost by act of law, as long as they have an exclusive right under the Postal Law, with their managing boards,

4. in the case of federal corporations, establishments and foundations under public law as well as associations of such corporations, establishments and foundations, with the managing board or the relevant representative body

and shall request a statement by a date which he shall determine. In the cases referred to in No. 4 of the first sentence above, the Federal Commissioner shall at the same time inform the competent supervisory authority.
(2) The Federal Commissioner may dispense with a complaint or with a statement from the body concerned especially if the irregularities involved are insignificant or have meanwhile been rectified.
(3) The statement to be delivered should also describe the measures taken as a result of the Federal Commissioner's complaint. The bodies referred to in sub-Section 1 first sentence No. 4 above shall submit to the competent supervisory authority a copy of the statement communicated to the Federal Commissioner.

Section 26
Further duties of the Federal Commissioner for Data Protection and Freedom of Information

(1) The Federal Commissioner for Data Protection and Freedom of Information shall submit an activity report to the Bundestag every two years. Such report should inform the Bundestag and the public on key developments in the field of data protection.
(2) When so requested by the Bundestag or the Federal Government, the Federal Commissioner shall draw up opinions and reports. When so requested by the Bundestag, the Petitions Committee, the Internal Affairs Committee or the Federal Government, the Federal Commissioner shall also investigate data protection matters and occurrences at public bodies of the Federation. The Federal Commissioner may at any time consult the Bundestag.
(3) The Federal Commissioner may make recommendations on the improvement of data protection to the Federal Government and to the bodies of the Federation referred to in Section 12 (1) of this Act and may advise them in matters regarding data protection. The bodies referred to in Nos. 1 to 4 of Section 25 (1) of this Act shall be informed by the Federal Commissioner when the recommendation or advice does not concern them directly.
(4) The Federal Commissioner shall seek cooperation with public bodies responsible for monitoring compliance with data protection provisions in the Länder and with supervisory authorities under Section 38 of this Act. Sentences 4 and 5 of Section 38 (1) shall apply mutatis mutandis.

Part III
Data processing by private bodies and public-law enterprises participating in competition

Chapter I
Legal basis for data processing

Section 27
Scope

(1) The provisions of this Part shall apply in so far as personal data are processed or used by means of data processing systems or collected for such purposes, or in so far as data are processed or used in or from automated filing systems or collected for such purposes by

1. private bodies,

2.

a) public bodies of the Federation in so far as they participate in competition as public-law enterprises,

b) public bodies of the Länder in so far as they participate in competition as public-law enterprises, execute federal law and data protection is not governed by Land legislation.

This shall not apply where the collection, processing or use of such data is effected solely for personal or family activities. In the cases referred to in No. 2 a) above, Sections 18, 21 and 24 to 26 shall apply instead of Section 38.

(2) The provisions of this Part shall not apply to the processing and use of personal data outside of non-automated filing systems in so far as they are not personal data clearly taken from an automated processing operation.

Section 28
Collection and storage of data for own commercial purposes

(1) The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible

1. when needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject,

2. in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use,

3. if the data are generally accessible or the controller of the filing system would be entitled to publish them, unless the data subject's legitimate interest in his data being excluded from processing or use clearly outweighs the justified interest of the controller of the filing system.

In connection with the collection of personal data, the purposes for which the data are to be processed or used are to be stipulated in concrete terms.

(2) Transfer or use for another purpose shall be admissible:

1. under the conditions given in sub-Section 1 first sentence No. 2 or No. 3,

2. where necessary

a) to protect the legitimate interests of a third party or

b) to avert threats to state or public security or to prosecute criminal offences,

and there is no reason to believe that the data subject has a legitimate interest in excluding transfer or use, or

3. if necessary in the interest of a research institute for the conduct of scientific research, if scientific interest in conduct of the research project substantially outweighs the interest of the data subject in excluding the change of purpose and if the research purpose cannot be attained by other means or can be attained thus only with disproportionate effort.

(3) The processing or use of personal data for purposes of advertising or trading in addresses shall be admissible if the data subject has provided consent and, if such consent was not provided in written form, if the controller proceeds in accordance with sub-Section 3a. In addition, processing or use of personal data shall be admissible where such data consist of lists or other summaries of data from groups of persons which are limited to the data subject's membership of this group, his/her occupation, name, title, academic degrees, address and year of birth and where processing or use is necessary

1. for advertising offers from the controller which collected the data, other than information concerning membership of the group, from the data subject in accordance with sub-Section 1 first sentence No. 1, or from generally accessible sources such as address, telephone and classified directories, and the like,

2. for purposes of advertising in view of the data subject's occupation and under his/her work address, or

3. for the purpose of soliciting donations eligible for tax concessions under Section 10 b (1) and Section 34 g of the Income Tax Act.

For purposes pursuant to sentence 2 No. 1, the controller may store data in addition to those stated there. Summarized personal data referred to in sentence 2 may be transferred for advertising purposes also when the transferred data are stored in accordance with Section 34 (1a) first sentence; in this case, the advertisement must make clear which body originally collected the data. Regardless of whether the conditions of sentence 2 are met, personal data may be used for advertising third-party offers if the data subject can clearly identify from the advertisement the body responsible for using the data. Processing or use as referred to in sentences 2 through 4 shall be admissible if not in conflict with legitimate interests of the data subject. Data transferred pursuant to sentences 1, 2 and 4 may be used only for the same purpose for which they were transferred.
(3a) If consent as referred to in Section 4 a (1) third sentence is provided in other than written form, the controller shall provide the data subject with written confirmation of the substance of the consent unless consent was provided in electronic form and the controller ensures that the declaration of con-sent is recorded and the data subject can access and revoke it at any time, to take future effect. If consent is provided in written form together with other declarations, the printing and format of the declaration shall distinguish it from the others.
(3b) The controller may not make the conclusion of a contract dependent on the data subject’s con-sent under sub-Section 3 first sentence if access to equivalent contractual benefits is impossible or unreasonable without providing consent. Consent provided under such circumstances shall be invalid.
(4) If the data subject objects vis-à-vis the controller of the filing system to the processing or use of his/her data for purposes of advertising or of market or opinion research, processing or use for such purposes shall be inadmissible. In approaching the data subject for the purpose of advertising or market or opinion research and, in the cases referred to in sub-Section 1 first sentence No. 1 also when creating a legal or quasi-legal obligation, the data subject shall be informed of the identity of the controller and the right of objections in accordance with sentence 1 above; in so far as the party approaching the data subject uses the data subject’s personal data which are stored by a body unknown to that party, the approaching party shall also ensure that the data subject is able to obtain information on the origin of the data. If the data subject objects to the processing or use of the data for the purpose of advertising or market or opinion research with the third party to whom the data were transferred for the purposes pursuant to sub-Section 3, the latter shall block the data for these purposes. In the cases of sub-Section 1 first sentence No. 1, the requirements as to the form of the objection cannot be stricter than for the creation of a legal or quasi-legal obligation.
(5) The third party to whom the data have been transferred may process or use the transferred data only for the purpose for which they were transferred. Processing or use for other purposes shall be admissible for private bodies only if the requirements of sub-sections 1 and 2 above are met and for public bodies only if the requirements of Section 14 (2) are met. The transferring body shall point this out to the third party.
(6) The collection, processing and use of special types of personal data (Section 3 (9)) for own commercial purposes shall be admissible when the data subject has not consented in accordance with Section 4a (3) if

1. this is necessary in order to protect vital interests of the data subject or of a third party, in so far as the data subject is unable to provide consent for physical or legal reasons,

2. the data concerned have evidently been made public by the data subject,

3. this is necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use, or

4. this is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project substantially outweighs the data subject's interest in excluding collection, processing and use and the purpose of the research cannot be achieved in any other way or would otherwise necessitate disproportionate effort.

(7) The collection of special types of personal data (Section 3 (9)) shall further be admissible if this is necessary for the purposes of preventive medicine, medical diagnosis, health care or treatment or the administration of health services and the processing of these data is carried out by medical personnel or other persons who are subject to an obligation to maintain secrecy. The processing and use of data for the purposes stated in sentence 1 shall be subject to the obligations to maintain secrecy which apply to the persons stated in sentence 1. The collection, processing or use of data on the health of persons by members of a profession other than those stipulated in Section 203 (1) and (3) of the Penal Code, the exercising of which profession involves determining, curing or alleviating illnesses or producing or selling aids shall be admissible only under those conditions according to which a doctor would also be authorized for these purposes.
(8) Special types of personal data (Section 3 (9)) may be transferred or used only if the requirements of sub-Section 6, Nos. 1 to 4 or sub-Section 7 first sentence are met. Transfer or use shall also be admissible if necessary to avert substantial threats to state security or public safety and to prosecute major criminal offences.
(9) Organizations of a political, philosophical or religious nature and trade union organizations may collect, process or use special types of personal data (Section 3 (9)) in so far as this is necessary for the organization's activities. This shall apply only to personal data of their members or of persons who maintain regular contact with the organizations in connection with the purposes of their activities. The transfer of these personal data to persons or bodies outside of the organization concerned shall be admissible only if the requirements of Section 4a (3) are met. Sub-Section 3, No. 2 shall apply mutatis mutandis.

Section 28a
Data transfer to credit inquiry agencies

(1) Personal data concerning a claim may be transferred to credit inquiry agencies only if the performance owed has not been rendered on time, the transfer is necessary to protect the justified interests of the controller or a third party and

1. the claim has been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedure,

2. the claim has been established under Section 178 of the Insolvency Act and has not been disputed by the debtor at the verification meeting,

3. the data subject has expressly acknowledged the claim,

4.

a) the data subject received at least two written reminders after the due date,

b) at least four weeks elapsed between the first warning and the data transfer,

c) the controller gave the data subject sufficient notice before transferring the information, or at least informed the data subject of the impending transfer in the first reminder and

d) the data subject did not dispute the claim, or

5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the controller has informed the data subject of the impending transfer.

The first sentence shall apply mutatis mutandis if the controller uses the data itself under Section 29.

(2) For the future transfer under Section 29 (2), financial institutions may transfer personal data on the creation, orderly execution and termination of a contractual relationship concerning a bank transaction under Section 1 (1) second sentence No. 2, No. 8 or No. 9 of the Banking Act to rating agencies unless the data subject's legitimate interest in excluding such transfer obviously outweighs the interest of the credit inquiry agency in the data. The data subject shall be informed of this before the contract has been concluded. The first sentence shall not apply to contracts concerning current accounts without overdraft protection. For the future transfer under Section 29 (2), data concerning the behaviour of data subjects which serve to create market transparency in the context of pre-contractual relationships of trust may not be transferred to credit inquiry agencies even with the data subject's consent.

(3) Within one month of becoming aware of any subsequent modification of facts based on a transfer under sub-Section 1 or 2, the controller shall inform the credit inquiry agency of such modification, as long as the credit inquiry agency is still storing the originally transferred data. The credit inquiry agency shall inform the body which transferred the data when it has erased the originally transferred data.

Section 28b
Scoring

For the purpose of deciding on the creation, execution or termination of a contractual relationship with the data subject, a probability value for certain future action by the data subject may be calculated or used if

1. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure,

2. in case the probability value is calculated by a credit inquiry agency, the conditions for transferring the data used under Section 29, and in all other cases the conditions of admissible use of data under Section 28 are met,

3. data in addition to address data are used to calculated the probability value,

4. in case address data are used, the data subject shall be notified ahead of time of the planned use of these data; this notification shall be documented.

Section 29
Commercial collection and storage of data for the purpose of transfer

(1) The commercial collection, storage, modification or use of personal data for the purpose of transfer, in particular when this serves the purposes of advertising, the activities of credit inquiry agencies or trading in addresses shall be admissible if

1. there is no reason to assume that the data subject has a legitimate interest in excluding such collection, storage or modification,

2. the data are retrievable from generally accessible sources or the controller would be permitted to publish them, unless the data subject clearly has an overriding legitimate interest in excluding such collection, storage or modification, or

3. the conditions of Section 28a (1) or (2) are met; data as defined in Section 28a (2) fourth sentence may not be collected or stored.

Section 28 (1) second sentence and sub-sections 3 to 3b shall be applied.
(2) Transfer for the purposes specified in sub-Section 1 shall be admissible if

1. the third party to whom the data are transferred credibly proves a justified interest in knowledge of the data and

2. there is no reason to assume that the data subject has a legitimate interest in his data being excluded from transfer.

Section 28 (3) to (3b) of this Act shall apply mutatis mutandis. In the case of transfer under sentence 1 No. 1 above, the reasons for the existence of a justified interest and the means of credibly presenting them shall be recorded by the transferring body. In the case of transfer through automated retrieval, such recording shall be required of the third party to whom the data are transferred. The transferring body shall take random samples in accordance with Section 10 (4) third sentence and thereby determine whether a legitimate interest exists.
(3) Personal data are not to be included in electronic or printed address, telephone, classified or similar directories if it is evident from the electronic or printed directory or register that such inclusion is contrary to the will of the data subject. The recipient of the data shall ensure that labels from electronic or printed directories or registers are retained upon adoption into directories or registers.
(4) Section 28 (4) and (5) shall apply to processing or use of the transferred data.
(5) Section 28 (6) to (9) shall apply mutatis mutandis.
(6) Any body which for the purpose of transfer commercially collects, stores or modifies personal data which may be used to evaluate the creditworthiness of consumers shall treat requests for in-formation from lenders in other European Union Member States or other states party to the Agreement on the European Economic Area the same way it treats information requests from do-mestic lenders.
(7) Anyone who refuses to conclude a consumer loan contract or a contract concerning financial assistance for payment with a consumer as the result of information provided by a body as referred to in sub-Section 6 shall immediate notify the consumer of this refusal and the information received. Such notification shall not be made if doing so would endanger public security or order. Section 6a shall remain unaffected.

Section 30
Commercial collection and storage of data for the purpose of transfer in anonymized form

(1) If personal data are collected and stored in the course of business in order to transfer them in anonymized form, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. Such characteristics may be combined with the information only where necessary for storage or scientific purposes.
(2) The modification of personal data shall be admissible if

1. there is no reason to assume that the data subject has a legitimate interest in his/her data being excluded from modification or

2. the data can be taken from generally accessible sources or the controller of the filing system would be entitled to publish them, unless the data subject clearly has an overriding legitimate interest in his/her data being excluded from modification.

(3) Personal data shall be erased if their storage is inadmissible.

(4) Section 29 shall not apply.
(5) Section 28 (6) to (9) shall apply mutatis mutandis.

Section 30a
Commercial data collection and storage for purposes of market or opinion research

(1) The commercial collection, processing or use of personal data for purposes of market or opinion research shall be admissible if

1. there is no reason to assume that the data subject has a legitimate interest in excluding such data from collection, processing or use, or

2. the data can be taken from generally accessible sources or the controller would be entitled to publish them and the data subject's legitimate interest in excluding such data from collection, processing or use does not obviously outweigh the interest of the controller.

Special types of personal data (Section 3 (9)) may be collected, processed or used only for certain research purposes.
(2) Personal data collected or stored for purposes of market or opinion research may be processed or used only for these purposes. Data which were not taken from generally accessible sources and which the controller is not entitled to publish may be processed or used only for the research project for which they were collected. They may be processed or used for another purpose only if they have been rendered anonymous in such a way that it is no longer possible to trace them to a specific person.
(3) Personal data shall be rendered anonymous as soon as allowed by the purpose of the research project for which they were collected. Until then, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. Such characteristics may be combined with the information only where necessary for the purpose of the research project.
(4) Section 29 shall not apply.
(5) Section 28 (4) and (6) to (9) shall apply mutatis mutandis.

Section 31
Limitation of use to specific purposes

Personal data stored exclusively for the purposes of data protection control or data security or to ensure the proper operation of a data processing system may be used only for these purposes.

Section 32
Data collection, processing and use for employment-related purposes

(1) Personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in excluding the collection, processing or use, and in particular the type and extent are not disproportionate to the reason.
(2) Sub-Section 1 shall also be applied when personal data are collected, processed or used without being processed by automatic procedures nor processed, used in or from a non-automated filing system, nor collected in such a filing system for the purpose of processing or use.
(3) The rights of participation of staff councils shall remain unaffected.

Chapter II
Rights of the data subject

Section 33
Notification of the data subject

(1) If personal data are stored for the first time for one's own purposes without the data subject's knowledge, the data subject shall be notified of such storage, the type of data, the purposes of collection, processing or use and the identity of the controller. If personal data are stored commercially without the data subject's knowledge for the purpose of transfer, the data subject shall be notified of their initial transfer and of the type of data transferred. In the cases covered by the first and second sentences above, the data subject shall also be notified of the categories of recipients, in so far as he/she cannot be expected to assume transfer to such recipients according to the circumstances of the individual case concerned.
(2) Notification shall not be required if

1. the data subject has received knowledge by other means of the storage or transfer of the data,

2. the data are stored merely because they may not be erased due to legal statutory or contractual provisions on their preservation or exclusively serve purposes of data security or data protection control and notification would require disproportionate effort.

3. the data must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding legal interest of a third party,

4. the law expressly provides for such storage or transfer,

5. storage or transfer is necessary for the purposes of scientific research and notification would require disproportionate effort,

6. the relevant public body has stated to the controller of the filing system that publication of the data would jeopardize public safety or order or would otherwise be detrimental to the Federation or a Land,

7. the data are stored for one's own purposes and

   a) are taken from generally accessible sources and notification is unfeasible on account of the large number of cases concerned or

   b) notification would considerably impair the business purposes of the controller of the filing system, unless the interest in notification outweighs such impairment, or

8. the data are stored commercially for the purpose of transfer and

   a) are taken from generally accessible sources in so far as they relate to those persons who published these data or

   b) the data are compiled in lists or otherwise combined (Section 29 (2), No. 1 (b) of this Act)

   and notification is unfeasible on account of the large number of cases concerned,

9. data taken from generally accessible sources stored commercially for purposes of market or opinion research and notification would not be feasible due to the large number of cases con-cerned.

The controller shall stipulate in writing under what conditions notification shall not be provided in accordance with sentence 1, Nos. 2 to 7.

Section 34
Provision of information to the data subject

(1) At the request of the data subject, the controller shall provide information

1. on stored data about the data subject, also where they refer to the origin of these data,

2. on the recipient or type of recipients to whom the data are provided, and

3. the reason for storage.

The data subject should provide a detailed description of the type of personal data he or she would like information about. If the personal data are commercially stored for the purpose of transfer, information about the origin and the recipients shall be provided even if this information is not stored. Information about the origin and recipients may be withheld if the interest in protecting trade secrets outweighs the data subject's interest in the information.
(1a) In the cases covered by Section 28 (3) fourth sentence, the transferring body shall store the origin of the data and the recipient for two years following the transfer and shall provide the data subject with information about the origin of the data and the recipient upon request. The first sentence shall apply to the recipient accordingly.
(2) In the cases covered by Section 28b, the decision-making body shall provide the data subject with the following information upon request:

1. probability values calculated or stored for the first time within the six months preceding the receipt of the information request,

2. the types of data used to calculate the probability values, and

3. how probability values are calculated and their significance, with reference to the individual case and in a form understandable to a general audience.

The first sentence shall apply mutatis mutandis when the decision-making body

1. stores the data used to calculate probability values without reference to specific persons but creates such reference when calculating the probability value, or

2. uses data stored by another body.

If a body other than the decision-making body calculated

1. the probability value or

2. one component of the probability value,

it shall provide the decision-making body at its request with the information necessary to satisfy the information claims under the first and second sentences. In the cases covered by sentence 3 No. 1, the decision-making body shall provide the data subject with the name and address of the other body as well as the information necessary to reference the individual case, so that the data subject may assert his/her claim to information, where the decision-making body does not provide this information itself. In this case, the body that calculated the probability value shall fulfil the data subject's request for information under the first and second sentences free of charge. The body responsible for calculating the probability value shall not be subject to the obligation referred to in the third sentence where the decision-making body uses its right under the fourth sentence.
(3) Any body which stores personal data commercially for the purpose of transfer shall provide the data subject upon request information about stored data concerning the data subject, even where these data are neither processed by automatic procedures nor stored in a non-automated filing system. The data subject shall be informed also about data
which currently have no reference to specific persons but for which the controller is to create such reference when responding to the information request,
which the controller does not store but uses for the purpose of providing information.
Information about the origin and recipients may be withheld if the interest in protecting trade secrets outweighs the data subject's interest in the information.

(4) Any body which collects, stores or modifies personal data commercially for the purpose of transfer shall provide the data subject upon request information about

1. probability values for certain future action by the data subject transferred within the twelve months preceding the receipt of the information request, as well as the names and last-known addresses of third parties to whom the values were transferred,

2. probability values at the time of the information request calculated according to the method used by the calculating body,

3. the types of data used to calculate the probability values under Nos. 1 and 2, and

4. how probability values are calculated and their significance, with reference to the individual case and in a form understandable to a general audience.

The first sentence shall apply mutatis mutandis when the responsible body

1. stores the data used to calculate probability values without reference to specific persons but creates such reference when calculating the probability value, or

2. uses data stored by another body.

(5) Data stored for the purpose of providing information to data subjects pursuant to sub-sections 1a to 4 may be used only for this purpose and for data protection control; they shall be blocked for other purposes.
(6) Upon request, the information shall be provided in written form, unless another form would be more appropriate in the circumstances.
(7) There shall be no obligation to provide information when the data subject does not have to be notified in accordance with Section 33 (2) first sentence Nos. 2, 3 and 5 to 7.
(8) The information shall be free of charge. If the personal data are stored commercially for the purpose of transfer, the data subject may request information in written form once per calendar year free of charge. For each additional request a fee may be charged, if the data subject can use the information for commercial purposes with respect to third parties. The fee may not exceed the direct costs of providing the information. No fee may be charged if

1. there is reason to believe that data are stored improperly or without permission, or

2. the information shows that the data are to be corrected under Section 35 (1) or to be erased under Section 35 (2) second sentence No. 1.

(9) If a fee is charged to provide information, the data subject shall be given the possibility of personal information about the data concerning him/her within the framework of his/her entitlement to information. The data subject shall be informed of this possibility.

Section 35
Correction, erasure and blocking of data

(1) Inaccurate personal data shall be corrected. Estimated data shall be clearly identified as such.
(2) Personal data may be erased at any time, except in the cases specified in sub-Section 3, Nos. 1 and 2. Personal data in filing systems shall be erased if

1. their storage is inadmissible,

2. they concern information on racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, sex life, criminal offences or administrative offences and the controller is unable to prove their accuracy,

3. they are processed for one’s own purposes, as soon as knowledge of them is no longer needed for fulfilling the purpose for which they are stored, or

4. they are processed commercially for the purpose of transfer and an examination at the end of the fourth calendar year, for data concerning matters that have been concluded and the data subject does not object at the end of the third calendar year after the data were first stored, if an examination shows that further storage is unnecessary.

Personal data stored on the basis of Section 28a (2) first sentence or Section 29 (1) first sentence No. 3 shall be erased at the data subject's request.
(3) Instead of erasure, personal data shall be blocked where

1. in the case of sub-Section 2 second sentence No. 3 above, retention periods prescribed by law, statutes or contracts rule out any erasure,

2. there is reason to assume that erasure would impair legitimate interests of the data subject or

3. erasure is not possible or is only possible with disproportionate effort due to the specific type of storage.

(4) Personal data shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect.
(4a) The fact that the data are blocked shall not be transmitted.
(5) Personal data must not be collected, processed or used for automated processing or processing in non-automated filing systems if the data subject files an objection with the controller and an examination reveals that the data subject's legitimate interest outweighs the controller's interest in such collection, processing or use, on account of the data subject's personal situation. Sentence 1 shall apply only when an obligation to carry out collection, processing or use is established by a legal provision.
(6) Where they are stored commercially for the purpose of transfer, personal data which are incorrect or whose accuracy is disputed need not be corrected, blocked or erased except in the cases mentioned in sub-Section 2, No. 2 above, if they are taken from generally accessible sources and are stored for documentation purposes. At the request of the data subject, his/her counter-statement shall be added to the data for the duration of their storage. The data may not be transferred without this counter-statement.
(7) The bodies to which data were transmitted for storage in the course of a data transfer process shall be notified of the correction of incorrect data, the blocking of disputed data and the erasure or blocking of data due to inadmissible storage, where this does not require disproportionate effort and the data subject has no overriding legitimate interests.
(8) Blocked data may be transferred or used without the consent of the data subject only if

1. this is indispensable for scientific purposes, for use as evidence or for other reasons in the overriding interests of the controller of the data or a third party and

2. transfer or use of the data for this purpose would be admissible if they were not blocked.

Chapter III
Supervisory authority

Section 36
Appointment of a data protection official

deleted

Section 38
Supervisory authority

(1) The supervisory authority shall monitor implementation of this Act and other data protection provisions governing the automated processing of personal data or the processing or use of personal data in or from non-automated filing systems, including the rights of the member states in the cases under Section 1 (5) of this Act. It shall advise and support the

data protection officials and the controllers with due regard to their typical requirements. The supervisory authority may process and use the data which it stores for supervisory purposes only; Section 14 (2), Nos. 1 to 3, 6 and 7 shall apply mutatis mutandis. The supervisory authority may, in particular, transfer data to other supervisory authorities for supervisory purposes. On request, it shall provide supplementary assistance to other Member States of the European Union (administrative assistance). If the supervisory authority establishes a breach of this Act or other data protection provisions, it shall be authorized to notify the data subjects accordingly, to report the breach to the bodies responsible for prosecution or punishment and, in cases of serious breaches, to notify the trade supervisory authority in order to initiate measures under industrial law. It shall publish an activity report on a regular basis, but at least every two years. Section 21 first sentence and Section 23 (5) sentences 4 to 7 shall apply mutatis mutandis.
(2) The supervisory authority shall keep a register of the automated processing operations which are subject to obligatory registration in accordance with Section 4d, stating the information specified in Section 4e first sentence. The register shall be open to inspection by any person. The right to inspection shall not extend to the information in accordance with Section 4e, sentence 1, No. 9 or stipulation of the persons entitled to access.
(3) The bodies subject to monitoring and the persons responsible for their management shall provide the supervisory authority on request and without delay with the information necessary for the performance of its duties. A person obliged to provide information may refuse to do so where he/she would expose himself or one of the persons designated in Section 383 (1), Nos. 1 to 3, of the Code of Civil Procedure to the danger of criminal prosecution or of proceedings under the Administrative Offences Act. This shall be pointed out to the person obliged to provide information.
(4) The persons appointed by the supervisory authority to exercise monitoring shall be authorized, where necessary for the performance of the duties of the supervisory authority, to enter the property and premises of the body during business hours and to carry out checks and inspections there. They may inspect business documents, especially the list stipulated in Section 4g (2) first sentence of this Act as well as the stored personal data and the data processing programs. Section 24 (6) of this Act shall apply mutatis mutandis. The person obliged to provide information shall permit such measures.
(5) To guarantee compliance with this Act and other data protection provisions, the supervisory authority may order measures to rectify violations during the collection, processing or use of personal data or technical or organizational irregularities detected. In the event of serious violations or irregularities, especially those connected with a special threat to privacy, the supervisory authority may prohibit collection, processing or use, or the use of particular procedures if the violations or irregularities are not rectified within a reasonable period contrary to the order pursuant to the first sentence above and despite the imposition of a fine. The supervisory authority may demand the dismissal of the data protection official if he/she does not possess the specialized knowledge and demonstrate the reliability necessary for the performance of his/her duties.
(6) The Land governments or the bodies authorized by them shall designate the supervisory authorities responsible for monitoring the implementation of data protection within the area of application of this Part.
(7) The Industrial Code shall continue to apply to commercial firms subject to the provisions of this Part.

Section 38a
Code of conduct to promote the implementation of data protection provisions

(1) Professional associations and other associations which represent specific groups of controllers may submit draft rules of conduct to promote the implementation of data protection provisions to the competent supervisory authority.
(2) The supervisory authority shall examine the compatibilty of the submitted drafts with the applicable law on data protection.

Part IV
Special provisions

Section 39
Limited use of personal data subject to professional or special official secrecy

(1) Personal data which are subject to professional or special official secrecy and which have been supplied by the body bound to secrecy in the performance of its professional or official duties may be processed or used by the controller of the filing system only for the purpose for which they were received. In the event of transfer to a private body, the body bound to secrecy must give its consent.
(2) The data may be processed or used for another purpose only if the change of purpose is permitted by special legislation.

Section 40
Processing and use of personal data by research institutes

(1) Personal data collected or stored for scientific research purposes may processed or used only for such purposes.
(2) The personal data shall be rendered anonymous as soon as the research purpose permits this. Until such time the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research purpose.
(3) Bodies conducting scientific research may publish personal data only if

1. the data subject has consented or
2. this is indispensable for the presentation of research findings on contemporary events.

Section 41
Collection, processing and use of personal data by the media

(1) The Länder are to ensure in their legislation that regulations corresponding to the provisions of Sections 5, 9 and 38a of this Act, including an appurtenant regulation on liability in accordance with Section 7 of this Act, shall apply to the collection, processing and use of personal data by enterprises or auxiliary enterprises in the press exclusively for their own journalistic-editorial or literary purposes.
(2) If journalistic-editorial processing or use of personal data by Deutsche Welle leads to the publication of counter-statements by the data subject, such counter-statements shall be combined with the stored data and preserved for the same period as the data themselves.
(3) If the privacy of a person is impaired by reporting by Deutsche Welle, he/she may request information on the stored personal data on which the reporting was based. Such information may be refused, after considering the legitimate interests of the parties concerned, in so far as

1. the data enable conclusions to be drawn as to the persons who are or have been professionally involved in a journalistic capacity in the preparation, production or dissemination of broadcasts,
2. the data enable conclusions to be drawn as to the supplier or source of contributions, documents and communications for the editorial part,
3. disclosure of the data obtained by research or other means would compromise Deutsche Welle's journalistic function by divulging its information resources.

The data subject may request that incorrect data be corrected.
(4) In all other respects, Sections 5, 7, 9 and 38a of this Act shall apply to Deutsche Welle. Instead of Sections 24 to 26 of this Act, Section 42 shall apply even where administrative matters are concerned.

Section 42
Data protection official of Deutsche Welle

(1) Deutsche Welle shall appoint a data protection official, who shall take the place of the Federal Commissioner for Data Protection and Freedom of Information. The data protection official shall be appointed by the board of administration for a term of four years upon nomination by the director-general; reappointments shall be admissible. The office of data protection official may be exercised alongside other duties within the broadcasting corporation.
(2) The data protection official shall monitor compliance with the provisions of this Act and with other provisions concerning data protection. He/she shall be independent in the exercise of this office and shall be subject to the law only. In all other respects he/she shall be subject to the official and legal authority of the board of administration.
(3) Anyone may appeal to the data protection official in accordance with Section 21 first sentence of this Act.
(4) The data protection official shall submit an activity report to the organs of Deutsche Welle every two years, beginning on 1 January 1994. In addition he/she shall submit special reports pursuant to a decision by an organ of Deutsche Welle. The data protection official shall forward the activity reports to the Federal Commissioner for Data Protection and Freedom of Information as well.
(5) Deutsche Welle shall make further arrangements for its area of activity in accordance with Sections 23 to 26 of this Act. Sections 4f and 4g of this Act shall remain unaffected.

Section 42a
Obligation to report unlawful access to data

If a private body as defined in Section 2 (4) or a public body as defined in Section 27 (1) first sentence No. 2 determines that

1. special types of personal data (Section 3 (9)),
2. personal data subject to professional secrecy,
3. personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or
4. personal data concerning bank or credit card accounts

stored with that body have been unlawfully transferred or otherwise unlawfully revealed to third parties, with the threat of serious harm to the data subject's rights or legitimate interests, then in accordance with sentences 2 to 5 the body shall notify the responsible supervisory authority and the data subject without delay. The data subject shall be notified as soon as appropriate measures have been taken to protect the data and notification would no longer put criminal prosecution at risk. The notification for the data subjects shall describe the nature of the unlawful access and include recommendations for measures to minimize possible harm. The notification for the competent supervisory authority shall also describe possible harmful consequences of the unlawful access and measures taken by the body. Where notifying the data subjects would require unreasonable effort, in particular due to the large number of cases involved, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying the data subjects. A notification distributed by the body required to provide notification may be used against that body in criminal proceedings or in proceedings in accordance with the Administrative Offences Act, or against an associate of the body required to provide notification as defined in Section 52 (1) of the Code of Criminal Procedure only with the consent of the body required to provide notification.

Part V
Final provisions

Section 43
Administrative offences

(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,

1. contrary to Section 4d (1), also in conjunction with Section 4e second sentence of this Act, fails to submit a notification, fails to do so within the prescribed time limit or fails to provide complete particulars,

2. contrary to Section 4f (1) first or second sentence of this Act, fails to appoint a data protection official or fails to do so within the prescribed time limit or in the prescribed manner,

2a. contrary to Section 10 (4) third sentence fails to ensure that data transfer can be ascertained and checked,

2b. contrary to Section 11 (2) second sentence fails to give the commission correctly, completely or in accordance with the rules, or contrary to Section 11 (2) fourth sentence fails to ensure prior to the processing of the data that technical and organizational measures taken by the agent are being complied with,

3. contrary to Section 28 (4) second sentence of this Act, fails to notify the data subject, or fails to do so within the prescribed time limit or in the prescribed manner, or fails to ensure that the data subject is able to obtain due knowledge,

3a. contrary to Section 28 (4) fourth sentence requires a stricter form,

4. transfers or uses personal data contrary to Section 28 (5) second sentence of this Act,

4a. contrary to Section 28a (3) first sentence fails to inform or fails to do so correctly, completely or within the prescribed time limits,

5. contrary to Section 29 (2) third or fourth sentence of this Act, fails to record the reasons described there or the means of credibly presenting them,

6. incorporates personal data into electronic or printed address, telephone, classified or similar directories contrary to Section 29 (3) first sentence of this Act,

7. contrary to Section 29 (3) second sentence of this Act, fails to ensure the adoption of labels,

7a. contrary to Section 29 (6) fails to handle an information request properly,

7b. contrary to Section 29 (7) first sentence fails to inform a consumer or fails to do so correctly, completely or within the prescribed time limits,

8. contrary to Section 33 (1) of this Act, fails to notify the data subject or fails to do so correctly or completely,

8a. contrary to Section 34 (1) first sentence, also in conjunction with sentence 3, contrary to Section 34 (1a), contrary to Section 34 (2) first sentence, also in conjunction with sentence 2, or contrary to Section 34 (2) fifth sentence, (3) first or second sentence, or (4) first sentence, also in conjunction with sentence 2 fails to provide information or fails to do so correctly, completely or within the prescribed time limits, or contrary to Section 34 (1a) fails to store data,

8b. contrary to Section 34 (2) third sentence fails to transmit information or fails to do so correctly, completely or within the prescribed time limits,

8c. contrary to Section 34 (2) fourth sentence fails to refer the data subject to the other body, or fails to do so within the prescribed time limits,

9. contrary to Section 35 (6) third sentence of this Act, transfers data without a counter-statement,

10. contrary to Section 38 (3) first sentence of this Act, fails to provide information or fails to do so correctly, completely or within the prescribed time limit or fails to permit a measure

11. fails to comply with an executable instruction under Section 38 (5) first sentence of this Act.

(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,

1. collects or processes personal data which are not generally accessible without authorization,

2. holds personal data which are not generally accessible ready for retrieval by means of an automated procedure without authorization,

3. retrieves personal data which are not generally accessible or obtains such data for themselves or another from automated processing operations without authorization,

4. obtains by means of incorrect information the transfer of personal data which are not generally accessible,

5. contrary to Section 16 (4) first sentence, Section 28 (5) first sentence of this Act, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1) of this Act, uses data for other purposes by transmitted them to third parties, or

5a. contrary to Section 28 (3b) makes concluding a contract dependent on the consent of the data subject,

5b. contrary to Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research,

6. contrary to Section 30 (1) second sentence, Section 30a (3) third sentence, Section 40 (2) third sentence of this Act, combines a characteristic mentioned there with specific information, or

7a. contrary to Section 42a first sentence fails to notify or fails to do so correctly, completely or within the prescribed time limit.

(3) Administrative offences shall be punishable by a fine of up to € 50,000 in case of sub-Section 1 above, and by a fine of up to € 300,000 in the cases under sub-Section 2 above. The fine shall exceed the financial benefit to the perpetrator derived from the administrative offence. If the amounts mentioned in the first sentence are not sufficient to do so, they may be increased.

Section 44
Criminal offences

(1) Anyone wilfully committing an offence specified in Section 43 (2) of this Act in exchange for payment or with the intention of enriching himself or another person or of harming another person shall be liable to imprisonment for up to two years or to a fine.
(2) Such offences shall be prosecuted only if a complaint is filed. Complaints may be filed by the data subject, the Federal Commissioner for Data Protection and Freedom of Information and the supervisory authority.

Part VI
Transitional provisions

Section 45
Current applications

Collections, processing or usages of personal data which have already begun on 23 May 2001 shall be harmonized with the provisions of this Act within three years of the aforesaid date. In so far as provisions of this Act are applied in legal provisions outside of the scope of application of directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, collections, processing or usages of personal data which have already begun on 23 May 2001 shall be harmonized with the provisions of this Act within five years of the aforesaid date.

Section 46
Overreaching validity of definitions

(1) Where the term "filing system" is employed in special legal provisions of the Federation, a filing system is

1. a set of personal data which can be evaluated according to specific characteristics by means of automated procedures (automated filing system) or
2. any other set of personal data which is similarly structured and can be arranged, rearranged and evaluated according to specific characteristics (non-automated filing system).

This shall not include files and sets of files, unless they can be rearranged and evaluated by means of automated procedures.
(2) Where the term "file" is employed in special legal provisions of the Federation, a file is any document serving official purposes which does not fall within the definition of a filing system as specified in sub-Section 1 above; this shall include image and sound recording media. It shall not include drafts and notes that are not intended to form part of a record.
(3) Where the term "recipient" is employed in special legal provisions of the Federation, a recipient is any person or body other than the controller. This shall not include the data subject or persons and bodies 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.

Section 47
Transitional provision

For the processing and use of data collected or stored prior to 1 September 2009, Section 28 of the version applicable up to that date shall continue to apply

1. to purposes of market or opinion research until 31 August 2010,
2. to advertising purposes until 31 August 2012.

Section 48
Report of the Federal Government

The Federal Government shall report to the Bundestag

1. until 31 December 2012 on the impacts of Sections 30a and 42a,
2. until 31 December 2014 on the impacts of the amendments to Sections 28 and 29.

If the Federal Government is of the view that legislative measures are advisable, the report shall contain a recommendation.

Annex
(to the first sentence of Section 9 of this Act)

Where personal data are processed or used automatically, the internal organization of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or data categories to be protected shall be taken,

1. to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control),

2. to prevent data processing systems from being used without authorization (access control),

3. to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control),

4. to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control),

5. to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control),

6. to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control),

7. to ensure that personal data are protected from accidental destruction or loss (availability control),

8. to ensure that data collected for different purposes can be processed separately.

One measure in accordance with the second sentence Nos. 2 to 4 is in particular the use of the latest encryption procedures.