Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)

Part I General provisions

Section 1 Purpose and scope
Section 2 Public and private bodies
Section 3 Further definitions
Section 4 Admissibility of data processing and use
Section 5 Confidentiality
Section 6 Inalienable rights of the data subject
Section 7 Compensation by public bodies
Section 8 Compensation by private bodies
Section 9 Technical and organizational measures
Section 10 Establishment of automated retrieval procedures
Section 11 Commissioned processing or use of personal data

Part II Data processing by public bodies

Chapter I Legal basis for data processing

Section 12 Scope
Section 13 Collection of data
Section 14 Storage, modification and use of data
Section 15 Communication of data to public bodies
Section 16 Communication of data to private bodies
Section 17 Communication of data to bodies outside the area of application of this Act
Section 18 Implementation of data protection in the federal administration

Chapter II Rights of the data subject

Section 19 Provision of information to the data subject
Section 20 Correction, erasure and blocking of data
Section 21 Appeals to the Federal Commissioner for Data Protection

Chapter III Federal Commissioner for Data Protection

Section 22 Election of the Federal Commissioner for Data Protection
Section 23 Legal status of the Federal Commissioner for Data Protection
Section 24 Monitoring by the Federal Commissioner for Data Protection
Section 25 Complaints lodged by the Federal Commissioner for Data Protection
Section 26 Further duties of the Federal-Commissioner for Data Protection; register of data files

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

Chapter I Legal basis for data processing

Section 27 Scope
Section 28 Storage, communication and use of data for own purposes
Section 29 Storage of data in the normal course of business for the purpose of communication
Section 30 Storage of data in the normal course of business for the purpose of communication in depersonalized form
Section 31 Limitation of use to specific purposes
Section 32 Obligatory registration

Chapter II Rights of the data subject

Section 33 Notification of the data subject
Section 34 Provision of information to the data subject
Section 35 Correction, erasure and blocking of data

Chapter III Data protection officer; supervisory authority

Section 36 Appointment of a data protection officer
Section 37 Duties of the data protection officer
Section 38 Supervisory authority

Part IV Special provisions

Section 39 Limited use of personal data subject to professional or special official secrecy
Section 40 Processing and use of personal data by research institutes
Section 41 Processing and use of personal data by the media
Section 42 Data protection officer at broadcasting corporations under federal law

Part V Final provisions

Section 43 Criminal offences
Section 44 Administrative offences

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

Data Protection in Germany

We live in an information society. Freely available information has become a new factor in the economy, indeed it is now among the most important factors of economic life. Data protection

actually means the right of the individual to have his personal data protected against unauthorised use. Data protection has developed in tandem with advances in electronic information technology since the early 1970s.

Modern technology has made it easier to handle information, with the result that the amount of information being processed has soared. It has become possible to collect, systematically access and pass on virtually unimaginable quantities of data at high speed. On the other hand, this ability can lead to problems as it is necessary to protect the privacy of the individual. In this sense, data protection is described as "one of the social limits that society has to impose on technological progress." The legal limits are provided by data protection law.

Data protection law was introduced in Germany about thirty years ago; it started in Hesse 1970. Since 1977 there has been a Federal Act. In 1983, Germany`s supreme court made a further milestone in the development. Since then the basic criterion for the handling of personal data by the public administration and by private data processors has been the right of the individual to determine the use of his own data. It is particularly important to guarantee the transparency of the movement of information. Therefore, key criteria for the handling of data are "necessity" and the "purpose limitation principle". Data protection led to a new constitutional right for the individual. The "right to be left alone", i.e. to pass on or withhold information, is a basic right which derives from the constitutional right to free development of the personality. Since the Federal Data Protection Act 1977 data processing is only permitted on the basis of statutory legislation with the agreement of the individual concerned. It has thus been made possible for the individual to keep track of his personal data.

The amended Data Protection Act of 1990 is also intended to protect the individual from having his personal rights infringed upon. The individual must consent to having his personal data collected or stored, or there must be a statutory arrangement. In general the state is not allowed to collect or store personal data without an individual consent; the main exemptions are in the fields of police investigations, intelligence services or defense. The data themselves are subject to data protection if they are not exclusively used in the private personal sphere.

Public-sector and private-sector agencies are required to inform the individual at his request about the data they hold on him.

The Federal Data Protection Act contains a number of security requirements restricting for example access to data processing facilities. Priorities lie increasingly on avoiding the storing of data and on promoting the use of it sparingly.

The Act has created the office of a Federal Data Protection Commissioner who is elected by the Bundestag. His main tasks are dealing with individual complaints and informing the plaintiff about the findings of his investigations, as well as giving recommendations to both parliament and the government.

A violation of data protection law can lead to prosecution. The offender can expect to be sentenced to imprisonment of between one year or to five years.

The European Data Protection Directive of 1995 ensured that data are protected in the same manner throughout the single European market. The Directive expands the rights of the individual to be informed and challenge the way his data are handled. The individual has the right to know which government agencies have access to which kind of personal data.

In 1980 an international basis was put in place by the OECD with a - non-binding - recommendation on "Guidelines for the protection of privacy and transponder flows of personal data". In 1990 the United Nations issued "Guidelines concerning computerized personal data", applied world-wide without being legally binding.

The organisation / structure of data protection in Germany

** The Federal Data Protection Act covers the data processing of all federal agencies including the federal government as well as the private sector.*

** 16 Data Protection Acts of the Länder cover the public sector data processing of the agencies of the Länder (e.g. counties, cities or universities).*

** Numerous special laws on the Federal and the level of the Länder regulate personal data processing and give competence to the supervisory institutions.*

** The Federal Data Protection Commissioner is responsible for the audits / controls of all federal agencies, all telecommunication services and all postal services.*

** 16 Commisioners of the Länder are responsible for the audits / controls of all agencies of the Länder and some of them (Berlin, Bremen, Hamburg and Lower Saxony) are also responsible for private sector agencies.*

** So-called supervisory authorities for data protection (Aufsichtsbehörde nach dem BDSG) are institutions of the Länder. They are responsible for controls of private sector agencies.*

Foreword provided by the Bundesbeauftragter für den Datenschutz

---

Part 1 General provisions

Section 1 Purpose and scope

(1) The purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his 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

3. private bodies in so far as they process or use data in or from data files in the normal course of business or for professional or commercial purposes.

(3) There shall be the following restrictions to the application of this Act:

1. Sections 5 and 9 only of this Act shall apply to automated data files that are temporarily set up exclusively for reasons of processing and are automatically erased after processing.

2. Sections 5, 9, 39 and 40 only of this Act shall apply to non-automated data files in which the personal data are not intended for communication to third parties. Furthermore, the regulations on the processing and use of personal data in records shall apply to the data files of public bodies. If personal data are communicated in a particular case, the provisions of this Act shall apply without restriction.

(4) 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.

(5) 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.

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 enterprises established by law out of the Special Fund of the German Ferderal Postal Administration are to be considered as public bodies, as long as they have an exclusive right according to the Postal Administration Law or the Telecommunication Installations Act.

(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 in so far as they are not covered by paragraphs 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) "Data file" means

1. a set of personal data which can be evaluated according to specific characteristics by means of automated procedures (automated data file) 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 data file).

This shall not include records and sets of records, unless they can be rearranged and evaluated by means of automated procedures.

(3) "Record" means any other document serving official purposes; 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.

(4) "Collection" means the acquisition of data on the data subject.

(5) "Processing" means the storage, modification, communication, 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. "communication" means the disclosure to a third party (recipient) of personal data stored or obtained by means of data processing either

a) through transmission of the data to the recipient by the controller of the data file or

b) through the recipient inspecting or retrieving data held ready by the controller of the data file 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.

(6) "Use" means any utilization of personal data other than processing.

(7) "Depersonalization" 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.

(8) "Controller of the data file" means any person or body storing personal data on his or its own behalf or commissioning others to store them.

(9) "third party" means any person or body other than the controller of the data file. This shall not include the data subject or persons and bodies commissioned to process or use personal data within the area of application of this Act.

Section 4 Admissibility of data processing and use

(1) The processing and use of personal data shall be admissible only if this Act or any other legal provision permits or prescribes them or if the data subject has consented.

(2) When consent is obtained from the data subject, he shall be informed of the purpose of storage and of any envisaged communication of his data and, at his 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, the declaration of consent shall be made distinguishable in its appearance.

(3) In the field of scientific research, a special circumstance pursuant to the second sentence of paragraph 2 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 the first sentence of paragraph 2 above and the reasons from which considerable impairment of the defined purpose of research would arise shall be recorded in writing.

Section 5 Confidentiality

Persons employed in data processing shall not 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 Inalienable rights of the data subject

(1) The data subject's right to information (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 in a data file which several bodies are entitled to store and if the data subject is unable to ascertain the controller of the data file, he may approach any of these bodies. Such body is obliged to forward the request of the data subject to the controller of the data file. The data subject shall be informed of the forwarding of the request and of the controller of the data file. 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 instead of the data subject. In such case the further procedure shall be as described in section 19 (6) of this Act.

Section 7 Compensation by public bodies

(1) Where a public body causes harm to the data subject through automated processing of his personal data that is inadmissible or incorrect under the provisions of this Act or other data protection provisions, such body is 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 paragraphs 1 and 2 above shall be limited to a total amount of DM 250,000. Where, due to the same occurrence, compensation has to be paid to several persons and exceeds the maximum amount of DM 250,000, the compensation paid to each of them shall be reduced in proportion to the maximum amount.

(4) If, in the case of a data file, several bodies are entitled to store the data and the injured person is unable to ascertain the controller of the data file, each body shall be liable.

(5) Where several parties are responsible they shall be jointly and severally liable.

(6) Sections 254 and 852 of the Civil Code shall apply mutatis mutandis to contributory negligence on the part of the data subject and to statutory limitation.

(7) Provisions according to which a party responsible is liable to a greater extent than under this provision or according to which another person is responsible for the harm shall remain unaffected.

(8) Recourse may be had to ordinary courts of law.

Section 8 Compensation by private bodies

If a data subject asserts a claim against a private body for compensation because of automated data processing that is inadmissible or incorrect under this Act or other data protection provisions and if it is disputed whether the harm caused results from a circumstance for which the controller of the data file is responsible, the burden of proof shall rest with the controller of the data file.

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 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. the data recipient,

3. the type of data to be communicated,

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 shall be notified of the establishment of retrieval procedures and of the specifications made under paragraph 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 ministers responsible for the controller of the data file 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 recipient. The controller of the data file shall examine the admissibility of retrieval only if there is cause for such examination. The controller of the data file shall ensure that the communication of personal data can be ascertained and checked at least by means of suitable sampling procedures. If all personal data are retrieved or communicated (batch processing), it shall be sufficient to ensure that the admissibility of the retrieval or communication of all data can be ascertained and checked.

(5) Paragraphs 1 to 4 above shall not apply to the retrieval of data that anybody may use either without or after special permission.

Section 11 Commissioned processing or use of personal data

(1) Where other bodies are commissioned to 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 to 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. The commission shall be given in writing, specifying the processing and use of the data, the technical and organizational measures and any subcommissions. In the case of public bodies, the commission may be given by the supervisory authority.

(3) The agent may process or use the data only as instructed by the principal. If he thinks that an instruction of the principal infringes this Act or other data protection provisions, he 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), (3) and (4) as well as sections 44 (1), Nos. 2, 5, 6 and 7 and (2) 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 process or use personal data in the normal course of business as service enterprises, sections 32, 36 to 38 of this Act.

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 17, 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 processed or used for the purpose of past, present or future service or employment contracts, section 28 (1) and (2), No. 1, as well as sections 33 to 35 of this Act shall apply instead of sections 14 to 17, 19 and 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.

(2) Personal data shall be collected from the data subject. They may be collected without his 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 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 with his knowledge, he shall be informed of the purpose of collection. If they 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. At his request he shall be informed of the legal provision and of the consequences of withholding particulars.

(4) 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.

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 data file 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 would withhold consent if he 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 can be taken from generally accessible sources or the controller of the data file would be entitled to publish them, unless the data subject clearly has an overriding legitimate interest in excluding the change of purpose,

6. this is necessary to avert substantial detriment to the common weal or any other immediate threat to public safety,

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 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.

(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 data file. This shall also apply to processing or

use for training and examination purposes by the controller of the data file, 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.

Section 15 Communication of data to public bodies

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

1. this is necessary for the performance of duties of the communicating body or the recipient and

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

(2) Responsibility for the admissibility of communication shall rest with the communicating body. If the data are communicated at the request of the recipient, the latter shall bear responsibility. In such case the communicating body shall merely examine whether the request for communication lies within the remit of the recipient, unless there is special reason to examine the admissibility of communication. Section 10 (4) of this Act shall remain unaffected.

(3) The recipient may process or use the communicated data for the purpose for which they were communicated. Processing or use for other purposes shall be admissible only if the requirements of section 14 (2) of this Act are met.

(4) Paragraphs 1 to 3 above shall apply mutatis mutandis to the communication of personal data to bodies of public-law religious societies, provided it is ensured that adequate data protection measures are taken by the recipient.

(5) Where personal data that may be communicated under paragraph 1 above are linked to other personal data of the data subject or a third party in records in such a way that separation is not possible or is possible only with unreasonable effort, communication 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) Paragraph 5 above shall apply mutatis mutandis if personal data are transmitted within a public body.

Section 16 Communication of data to private bodies

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

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

2. the recipient credibly proves a justified interest in knowledge of the data to be communicated and the data subject does not have a legitimate interest in excluding their communication.

(2) Responsibility for the admissibility of communication shall rest with the communicating body.

(3) In cases of communication under paragraph 1, No. 2 above, the communicating body shall inform the data subject of the communication of his data. This shall not apply if it can be assumed that he will acquire knowledge of such communication in another manner or if such information would jeopardize public safety or otherwise be detrimental to the Federation or a Land.

(4) The recipient may process or use the communicated data only for the purpose for which they were communicated to him. The communicating body shall point this out to the recipient. Processing or use for other purposes shall be admissible if communication under paragraph 1 above would be admissible and the communicating body has consented.

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

(1) Section 16 (1) of this Act in conjunction with the relevant laws and agreements as well as section 16 (3) of this Act shall apply to the communication of personal data to bodies outside the area of application of this Act and to supranational or international bodies.

(2) Communication shall not occur where there is reason to assume that this would be incompatible with the purpose of a German law.

(3) Responsibility for the admissibility of communication shall rest with the communicating body.

(4) It shall be pointed out to the recipient that the communicated data may be processed or used only for the purpose for which they were communicated to him.

Section 18 Implementation of data protection in the federal administration

(1) Supreme Federal Authorities, the President of the Federal Railway Special Fund as well as direct bodies, establishments and foundations of public law subject merely to legal supervision by the Federal Government or a supreme Federal Authority have to ensure the implementation of this Act and other legal data protection provisions in their respective areas of activity.

The same applies to the Board of Directors of the enterprises established by law out of the Special Fund of the German Federal Postal Administration, as long as they have an exclusive right according to the Postal Administration Law or the Telecommunication Installation Act.

(2) Public bodies shall keep a register of the data processing systems used. In respect of their data files they shall record the following in writing:

1. designation and type of data files,

2. purpose,

3. type of data stored,

4. data subjects,

5. type of data to be communicated regularly and their recipients,

6. standard periods for the erasure of data,

7. groups of persons entitled to access or persons exclusively entitled to access.

They shall also ensure that the proper use of data processing programs by means of which personal data are to be processed is monitored.

(3) The second sentence of paragraph 2 above shall not apply to data files which are kept only temporarily and are erased within three months of being set up.

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 or recipient, and

2. 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 in records, 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 of the data file shall exercise due discretion in determining the procedure for providing such information and, in particular, the form in which it is provided.

(2) Paragraph 1 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 preservation or exclusively serve purposes of data security or data protection control.

(3) If the provision of information relates to the communication 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 of the data file,

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 may appeal to the Federal Commissioner for Data Protection.

(6) If no information is provided to the data subject, it shall at his request be supplied to the Federal Commissioner for Data Protection, unless the relevant supreme federal authority determines in a particular case that this would jeopardize the security of the Federation or a Land. The communication 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 of the data file, unless the latter consents to more extensive information being provided.

(7) Information shall be provided free of charge.

Section 20 Correction, erasure and blocking of data

(1) Incorrect personal data shall , be corrected. If it is ascertained that personal data in records are incorrect or if the data subject disputes that they are correct, a note to this effect shall be made in the record or it shall be recorded by some other means.

(2) Personal data in data files shall be erased if

1. their storage is inadmissible or

2. knowledge of them is no longer required by the controller of the data file for the performance of his duties.

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

1. preservation 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 in data files 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 in records shall be blocked if the authority ascertains in the particular case that, without blocking, legitimate interests of the data subject would be impaired and the data are no longer required for the performance of the authority's duties.

(6) Blocked data may be communicated 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 file or a third party and

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

(7) If necessary to protect legitimate interests of the data subject, 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 communication.

(8) 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

Anyone may appeal to the Federal Commissioner for Data Protection if he believes that his rights have been infringed through the collection, processing or use of his 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

Section 22 Election of the Federal Commissioner for Data Protection

(1) On a proposal from the Federal Government the Bundestag shall elect the Federal Commissioner for Data Protection 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 it 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 shall be independent in the performance of his duties and subject to the law only. He 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 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 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 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

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

1. on expiry of his term of office;

2. on his dismissal.

The Federal President shall dismiss the Federal 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 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 official duties and shall not belong to the management, supervisory boa rd or boa rd of directors of a profit-making enterprise nor to a government or a legislative body of the Federation or a Land. He may not deliver extrajudicial opinions in exchange for payment.

(3) The Federal Commissioner shall inform the Federal Minister of the Interior of any gifts that he receives in the performance of his duties. The Federal Minister of the Interior shall decide how such gifts shall be used.

(4) The Federal Commissioner shall be entitled to refuse to give testimony as a witness on persons who have entrusted information to him in his 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 may not be required to submit or surrender records or other documents.

(5) The Federal Commissioner shall be obliged, even after termination of his service, to maintain secrecy concerning information of which he has knowledge by reason of his duties. This shall not apply to communications made in the normal course of duties or concerning facts which are common knowledge or are not sufficiently important to warrant confidential treatment. The Federal 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 Minister of the Interior. This provision shall not, however, affect his duty by law to report criminal offences and to take action to uphold the free democratic fundamental order whenever it is jeopardized.

(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, as published on 12 December 1985 (Federal Law Gazette I, p. 2229), shall remain unaffected.

(7) From the beginning of the calendar month in which he commences his duties until the end of the calendar month in which he terminates his duties or, in the event of the sixth sentence of paragraph 1 above being applied, until the end of the month in which his 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, sections 13 to 20 of the Act on Federal Ministers, as published on 27 July 1971 (Federal Law Gazette I , p. 1166) and last amended by the Act of 22 December 1982 Reducing the Remuneration of Members of the Federal Government and Parliamentary State Secretaries (Federal Law Gazette I, p. 2007), shall apply, except that the period of office of two years provided in section 15 (1) of the Act on Federal Ministers shall be replaced by a period of office of five years. Notwithstanding the third sentence above in conjunction with sections 15 to 17 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 election, the Federal Commissioner held as civil servant or judge at least the last position customarily required before reaching the B 9 pay grade.

Section 24 Monitoring by the Federal Commissioner for Data Protection

(1) The Federal Commissioner for Data Protection shall monitor compliance with the provisions of this Act and other data Protection provisions by public bodies of the Federation. Where personal data in records are processed or used, the Federal Commissioner shall monitor their collection, processing or use if the data subject adequately indicates that his rights have been infringed in this respect or if the Federal Commissioner has in his possession adequate indications of such infringement.

(2) Monitoring by the Federal Commissioner shall also extend to personal data subject to professional or special official secrecy, especially tax secrecy under section 30 of the Tax Code. In the case of the Federal Authorities within the meaning of section 2 para. (1) sentence 2 the mail and telecommunication secrecy (Section 10 Basic Law) shall be restricted, as long as it is necessary for the exercise of supervision of the controller of the data file. Except as provided in No. 1 below, the right of monitoring shall not extend to the contents of posts and telecommunications. The following shall not be subject to monitoring by the Federal Commissioner:

1. personal data subject to monitoring by the commission set up under section 9 of the Act Implementing Article 10 of the Basic Law, 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, and

(a) personal data subject to privacy of posts and telecommunications under article 10 of the Basic Law,

(b) personal data subject to medical privacy and

(c) personal data in personnel or vetting records,

if the data subject objects in a particular case vis-à-vis the Federal Commissioner for Data Protection to the monitoring of data relating to him. Without prejudice to the Federal

Commissioner's right of monitoring, the public body shall inform data subjects in a general form of their right of objection.

(3) Federal courts shall be subject to monitoring by the Federal Commissioner only where they deal with administrative matters.

(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 and records, especially stored data and data processing programs, connected with the monitoring referred to in paragraph 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 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) Paragraph 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

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

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

2. in the case of the German Federal Railways, with the managing board,

3. in the case of the enterprises established by law out of the Special Fund of the German Federal Postal Administration, as long as they have an exclusive right vis à vis their Boards of directors according to the Postal Administration Law or the Telecommunication Installation Act,

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 No. 4 of the first sentence of paragraph 1 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; register of data files

(1) The Federal Commissioner for Data Protection shall submit an activity report to the Bundestag every two years. Such report should also contain a description of the main developments concerning data protection in the private sector.

(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.

(5) The Federal Commissioner shall keep a register of automatically operated data files in which personal data are stored. This shall not apply to the data files of the authorities referred to in section 19 (3) of this Act and to data files under section 18 (3) of this Act. The public bodies whose data files are included in the register shall be obliged to submit to the Federal Commissioner a list in accordance with Nos. 1 to 6 of the second sentence of section 18 (2) of this Act. The register shall be open to inspection by any person. The information under

Nos. 3 and 5 of the second sentence of section 18 (2) of this Act concerning data files of the authorities referred to in section 6 (2) of this Act shall not be subject to inspection. In particular cases the Federal Commissioner may agree with other public bodies that specific information is not subject to inspection.

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

Chapter 1 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 in or from data files in the normal course of business or for professional or commercial 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.

In the cases referred to in No. 2 (a) above, sections 18, 21 and 24 to 26 of this Act shall apply instead of section 38.

(2) The provisions of this Part shall not apply to the processing and use of personal data in records in so far as they are not personal data clearly taken from a data file.

Section 28 Storage, communication and use of data for own purposes

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

1. in accordance with the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject,

2. in so far as this is necessary to safeguard justified interests of the controller of the data file 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 can be taken from generally accessible sources or the controller of the data file would be entitled to publish them, unless the data subject clearly has an overriding legitimate interest in his data being excluded from processing or use,

4. if this is necessary in the interest of the controller of the data file 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.

The data must be obtained fairly and lawfully.

(2) Communication or use shall also be admissible

1. a) in so far as this is necessary to safeguard justified interests of a third party or public interests or

b) if the data, compiled in lists or otherwise combined, concern members of a group of persons and are restricted to

- the data subject's membership of this group of persons,

- occupation or type of business,

- name,

- title,

- academic degrees,

- address,

- year of birth

and if there is no reason to assume that the data subject has a legitimate interest in his data

being excluded from communication. In the cases under (b) above it can generally be assumed that such interest exists where data are to be communicated which were stored for the purposes of a contract or a quasi-contractual fiduciary relationship and which concern

- health matters,

- criminal offences,

- administrative offences,

- religious or political views and

- when communicated by the employer, to the legal status under labour law or

2. if this is 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) If the data subject objects vis-à-vis the controller of the data file to the use or communication of his data for purposes of advertising or of market or opinion research, use or communication for such purposes shall be inadmissible. Where the data subject objects vis-à-vis the recipient of data communicated under paragraph 2 above to processing or use for purposes of advertising or of market or opinion research, the recipient shall block the data for such purposes.

(4) The recipient may process or use the communicated data for the purpose for which they were communicated to him. Processing or use for other purposes shall be admissible only if the requirements of paragraphs 1 and 2 above are met. The communicating body shall point this out to the recipient.

Section 29 Storage of data in the normal course of business for the purpose of communication

(1) The storage or modification of personal data in the normal course of business for the purpose of communication shall be admissible if

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

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

The second sentence of section 28 (1) of this Act shall apply.

(2) Communication shall be admissible if

1. a) the recipient credibly proves a justified interest in knowledge of the data or

b) the data pursuant to section 28 (2), No. 1 (b) of this Act have been compiled in lists or otherwise combined and are to be communicated for purposes of advertising or of market or opinion research and

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

The second sentence of section 28 (2), No. 1 of this Act shall apply mutatis mutandis. In the case of communication under No. 1 (a) above, the reasons for the existence of a justified interest and the means of credibly presenting them shall be recorded by the communicating body. In the case of communication through automated retrieval, such recording shall be required of the recipient.

(3) Section 28 (3) and (4) of this Act shall apply to the processing or use of communicated data.

Section 30 Storage of data in the normal course of business for the purpose of communication in depersonalized form

(1) If personal data are stored in the normal course of business in order to communicate them in depersonalized 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 data being excluded from modification or

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

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

(4) Sections 29, 33 to 35 of this Act shall not apply.

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 Obligatory registration

(1) Bodies which in the normal course of business

1. store personal data for the purpose of communication,

2. store personal data for the purpose of depersonalized communication or

3. are commissioned to process or use personal data as a service enterprise

as well as their branches and dependent offices shall notify the commencement and termination of their activities to the relevant supervisory authority within one month.

(2) Upon registration, the following particulars shall be supplied for the register kept by the supervisory authority:

1. name or title of the body,

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

3. address,

4. business purposes of the body and of data processing,

5. name of the data protection officer,

6. General description of the type of personal data stored. This information shall not be required in the case of paragraph 1, No. 3, above.

(3) Upon registration, the following particulars which shall not be included in the register shall also be supplied:

1. type of data processing systems used,

2. in the event of regular communication of personal data, the recipients and type of data communicated.

(4) Paragraph 1 above shall apply mutatis mutandis to the change of particulars supplied in accordance with paragraphs 2 and 3 above.

(5) The supervisory authority may determine in a particular case which particulars have to be supplied in accordance with paragraph 2, Nos. 4 and 6, paragraph 3 and paragraph 4 above. The effort connected with the supply of these particulars must be in reasonable proportion to their significance for monitoring by the supervisory authority.

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, the data subject shall be notified of such storage and of the type of data. If personal data are stored in the normal course of business for the purpose of communication, the data subject shall be notified of their initial communication and of the type of data communicated.

(2) Notification shall not be required if

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

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

5. the data are stored in a data file which is kept only temporarily and is erased within three months of being set up,

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

a) are taken from generally accessible sources or

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

7. the data are stored in the normal course of business for the purpose of communication 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)

Section 34 Provision of information to the data subject

(1) The data subject may request information on

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

2. the purpose of storage and

3. persons and bodies to whom his data are regularly communicated if his data are processed automatically.

He should specify the type of personal data on which information is to be provided. If the personal data are stored in the normal course of business for the purpose of communication, the data subject may request information on their origin and recipient only if he has well-founded doubts about the correctness of the data. In such case, information on the origin and recipient shall be provided even if these particulars are not stored.

(2) In the case of bodies which store personal data in the normal course of business for the purpose of supplying information, the data subject may request information on his personal data even if they are not stored in a data file. The data subject may request information on their origin and recipient only if he proves that he has well-founded doubts about the correctness of the data. Section 38 (1) of this Act shall apply on condition that the supervisory authority checks in the particular case compliance with the first sentence above if the data subject gives reasons proving that the information was not provided or was provided incorrectly.

(3) Information shall be provided in writing unless special circumstances warrant any other form.

(4) The provision of information shall not be required if the data subject does not have to be notified in accordance with section 33 (2), Nos. 2 to 6, of this Act.

(5) Information shall be provided free of charge. However, if the personal data are stored in the normal course of business for the purpose of communication, a fee may be charged if the data subject can use the information vis-à-vis third parties for commercial purposes. The fee shall not exceed the costs directly attributable to the provision of information. No fee may be charged in cases where special circumstances give rise to the assumption that stored personal data are incorrect or that their storage was inadmissible, or where the information has revealed that the personal data have to be corrected or, subject to No. 1 of the second sentence of section 35 (2) of this Act, have to be erased.

(6) Where information is not provided free of charge, the data subject shall be given the possibility to acquire personal knowledge of the data and particulars concerning him within the framework of his entitlement to information. This shall be pointed out to him in a suitable manner.

Section 35 Correction, erasure and blocking of data

(1) Incorrect personal data shall be corrected.

(2) Apart from the cases mentioned in paragraph 3, Nos. 1 and 2, below personal data may be erased at any time. They shall be erased if

1. their storage is inadmissible,

2. they relate to health matters, criminal offences, administrative offences as well as religious or political views and the controller of the data file cannot prove that they are correct,

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 in the normal course of business for the purpose of communication and an examination five calendar years after their first being stored shows that further storage is not necessary.

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

1. in the case of paragraph 2, No. 3 or 4 above, preservation 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.

(5) Where they are stored in the normal course of business for the purpose of communication, personal data which are incorrect or whose correctness is disputed need not be corrected, blocked or erased except in the cases mentioned in paragraph 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 counterstatement shall be added to the data for the duration of their storage. The data may not be communicated without this counter-statement.

(6) If necessary to protect legitimate interests of the data subject, 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 communication.

(7) Blocked data may be communicated 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 file or a third party and

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

Chapter III Data protection officer; supervisory authority

Section 36 Appointment of a data protection officer

(1) Private bodies which process personal data automatically and regularly employ at least five permanent employees for this purpose shall appoint in writing a data protection officer

within one month of the commencement of 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.

(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 officer.

(3) The data protection officer shall be directly subordinate to the owner, managing board, managing director or other lawfully or constitutionally appointed manager. He shall be free to use his specialized knowledge in the area of data protection at his own discretion. He shall suffer no disadvantage through the performance of his duties. The appointment of a data protection officer may only be revoked at the request of the supervisory authority or by section 626 of the Civil Code being applied mutatis mutandis.

(4) The data protection officer 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 is released from this obligation by the data subject.

(5) The private body shall support the data protection officer in the performance of his duties and in particular, to the extent needed for such performance, make available assistants as well as premises, furnishings, equipment and other resources.

Section 37 Duties of the data protection officer

(1) The data protection officer shall be responsible for ensuring that this Act and other provisions concerning data protection are observed. For this purpose he may apply to the supervisory authority in cases of doubt. 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 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, with particular reference to the situation prevailing in this area and the special data protection requirements arising therefrom;

3. assist and advise in the selection of persons to be employed in the processing of personal data.

(2) The data protection officer shall receive from the private body a list on

1. data processing systems used,

2. designation and type of data files,

3. type of data stored,

4. business purposes the fulfilment of which necessitate a knowledge of these data,

5. their regular recipients,

6. groups of persons entitled to access or persons exclusively entitled to access.

(3) Paragraph 2, Nos. 2 to 6 above shall not apply to data files which are kept only temporarily and are erased within three months of being set up.

Section 38 Supervisory authority

(1) The supervisory authority shall check in a particular case that this Act and other data protection provisions governing the processing or use of personal data in or from data files are observed if it possesses sufficient indications that any such provision has been violated by private bodies, especially if the data subject himself submits evidence to this effect.

(2) If personal data are in the normal course of business

1. stored for the purpose of communication,

2. stored for the purpose of depersonalized communication or

3. processed by service enterprises commissioned to do so,

the supervisory authority shall monitor observance of this Act or other data protection provisions governing the processing or use of personal data in or from data files. The supervisory authority shall keep a register in accordance with section 32 (2) of this Act. The register shall be open to inspection by any person.

(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 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, in so far as 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 under section 37 (2) 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 data protection under this Act and other data protection provisions governing the processing or use of personal data in or from data files, the supervisory authority may instruct that, within the scope of the requirements set out in section 9 of this Act, measures be taken to rectify technical or organizational irregularities discovered. In the event of grave irregularities of this kind, especially where they are connected with a specific impairment of privacy, the supervisory authority may prohibit the use of particular procedures if the irregularities are not rectified within a reasonable period contrary to the instruction pursuant to the first sentence above and despite the imposition of a fine. The supervisory authority may demand the dismissal of the data protection officer if he does not possess the specialized knowledge and demonstrate the reliability necessary for the performance of his 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.

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 data file only for the purpose for which he has received them. In the event of communication 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 be processed or used only for such purposes.

(2) The communication of personal data to other than public bodies for scientific research purposes shall be admissible only if these undertake not to process or use the communicated data for other purposes and to comply with the provisions of paragraph 3 below.

(3) The personal data shall be depersonalized 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.

(4) 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 Processing and use of personal data by the media

(1) Where personal data are processed or used by enterprises or auxiliary enterprises in the press or film sector or by auxiliary enterprises in the broadcasting sector exclusively for their own journalistic - editorial purposes, only sections 5 and 9 of this Act shall apply. Where publishing houses process or use personal data for the publication of address, telephone, classified or similar directories, the first sentence above shall apply only if a journalistic - editorial activity is connected with such publication.

(2) If journalistic - editorial processing or use of personal data by broadcasting corporations under federal law 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 broadcasting corporations under federal law, he may request information on the stored personal data on which the reporting was based. Such information may be refused where the data enable conclusions to be drawn as to the author, supplier or source of contributions, documents and communications for the editorial part. The data subject may request that incorrect data be corrected.

(4) In all other respects, sections 5 and 9 of this Act shall apply to broadcasting corporations under federal law. Instead of sections 24 to 26 of this Act, section 42 shall apply even where administrative matters are concerned.

Section 42 Data protection officer at broadcasting corporations under federal law

(1) Broadcasting corporations under federal law shall each appoint a data protection officer, who shall take the place of the Federal Commissioner for Data Protection. The data protection officer 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 officer may be exercised alongside other duties within the broadcasting corporation.

(2) The data protection officer shall monitor compliance with the provisions of this Act and with other provisions concerning data protection. He shall be independent in the exercise of this office and shall be subject to the law only. In all other respects he shall be subject to the official and legal authority of the board of administration.

(3) Anyone may appeal to the data. protection officer in accordance with the first sentence of section 21 of this Act.

(4) The data protection officer shall submit an activity report to the organs of the respective broadcasting corporation under federal law every two years, beginning on 1 January 1994. In addition he shall- submit special reports pursuant to a decision by an organ of the respective broadcasting corporation. The data protection officer shall transmit the activity reports to the Federal Commissioner for Data Protection as well.

(5) Broadcasting corporations under federal law shall make further arrangements for their area of activity in accordance with sections 23 to 26 of this Act. Section 18 of this Act shall remain unaffected.

Part V Final provisions

Section 43 Criminal offences

(1) Anyone who, without authorization,

1. stores, modifies or communicates,

2. makes available for automatic retrieval or

3. retrieves or obtains for himself or for others from data files

any personal data protected by this Act which are not common knowledge shall be punished by imprisonment for up to one year or by a fine.

(2) Likewise punishable shall be anyone who

1. obtains by means of incorrect information the communication of personal data protected by this Act which are not common knowledge,

2. contrary to the first sentence of section 16 (4), the first sentence of section 28 (4), also in conjunction with section 29 (3), the first sentence of section 39 (1) or section 40 (1) of this Act, uses the communicated data for other purposes by transmitting them to third parties or

3. contrary to the second sentence of section 30 (1) of this Act, combines the characteristics mentioned in the first sentence of section 30 (1) with the information or, contrary to the third sentence of section 40 (3), combines the characteristics mentioned in the second sentence of section 40 (3) with the information.

(3) Where the offender commits the offence in exchange for payment or with the intention of enriching himself or another person or of harming another person, he shall be liable to imprisonment for up to two years or to a fine.

(4) Such offences shall be prosecuted only if a complaint filed.

Section 44 Administrative offences

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

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

2. contrary to section 32 (1), also in conjunction with section 32 (4) of this Act, fails to submit a notification or fails to do so within the prescribed time limit or, contrary to section 32 (2), also in conjunction with section 32 (4) of this Act, falls, when registering, to provide the required particulars or to provide correct or complete particulars,

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

4. contrary to the third sentence of section 35 (5) of this Act, communicates data without a

counter-statement,

5. contrary to section 36 (1) of this Act, fails to appoint a data protection officer or fails to do so within the prescribed time limit,

6. contrary to the first sentence of section 38 (3) of this Act, fails to provide information or fails to do so correctly, completely or within the prescribed time limit or, contrary to the fourth sentence of section 38 (4) of this Act, refuses to grant access to property or premises or refuses to permit checks or inspections or the inspection of business documents, or

7. fails to comply with an executable instruction under the first sentence of section 38 (5) of this Act.

(2) Such administrative offences shall be punishable by a fine of up to DM 50,000.

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

Where personal data are processed automatically, measures suited to the type of personal data to be protected shall be taken

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

2. to prevent storage media from being read, copied, modified or removed without, authorization (storage media control),

3. to prevent unauthorized input into the memory and the unauthorized examination, modification or erasure of stored personal data (memory control),

4. to prevent data processing systems from being used by unauthorized persons with the aid of data transmission facilities (user control),

5. 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 (access control),

6. to ensure that it is possible to check and establish to which bodies personal data can be communicated by means of data transmission facilities (communication control)

7. to ensure that it is possible to check and establish which personal data have been input into data processing systems by whom and at what time (input control),

8. 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) ,

9. to prevent data from being read, copied, modified or erased without authorization during the transmission of personal data or the transport of storage media (transfer control),

10. to arrange the internal organization of authorities or enterprises in such a way that it meets the specific requirements of data protection (organizational control) .