FEDERAL DATA PROTECTION ACT

of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325), law of December 16, 1997 (BGBl. I S. 2325) and December 17, 1997 (BGBl. I S. 2325), last amendment by law of May 23, 2001

Part 1. General and common 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 with administrative matters.

    3. non-public bodies, where they process, use or collect the data by means of or for data processing systems or where they process, use or collect the data in or from or for non-automated filing systems, unless the collection, processing or use of the data is solely for personal or domestic 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 have no application where a data controller located in another Member State of the European Union or in another contracting state to the Agreement on the European Economic Area collects, processes or uses personal data in Germany, unless this is carried out by a German branch. This Act shall apply where a data controller which is not located in a Member State of the European Union or in another contracting state to the Agreement on the European Economic Area collects, processes or uses personal data in Germany. Where this Act requires the data controller to be named, particulars shall also be required of its representative based in Germany. The previous two sentences shall not apply where data media are used only for the purpose of transit through Germany. The first sentence of §38, paragraph

(1), is 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 enterprises established by law out of the Special Fund of the German Federal Postal Administration are to be considered as public bodies, as long as they have an exclusive right according to the Postal Administration 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 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. Automatic processing means the collection, processing or use of personal data by means of data-processing equipment. A non-automated filing system is any non-automated set of personal data which is uniformly structured and can be accessed and evaluated according to specified characteristics.

3. "Collection" means the acquisition of data on the data subject.

4. "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 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 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.

5. "Use" means any utilization of personal data other than processing.

6. "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.

   (6a) Pseudonymisation means the replacement of the name and other identifying attributes with a code with a view to making it impossible or significantly more difficult to identify the data subject.

7. Data controller means any person or body which collects, processes or uses personal data for itself or which engages others to do so on its behalf.

8. Recipient means any person or body which receives data. Third party means any person or body other than the data controller. Third party does not include the data subject or persons and bodies in another Member State of the European Union or in another contracting state to the Agreement on the European Economic Area which collect, process or use data on behalf of others.

9. Special categories of personal data means data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual life.

10. Mobile personal recording and processing media are data media,

    1. which are supplied to the data subject,

    2. on which personal data can be automatically processed, other than mere recording, by the supplying body or by another body and

    3. where the data subject can influence this processing only by using the medium.

Section 3a. Data avoidance and data economy ➦

The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected.

Section 4. Lawfulness of data collection, processing and use ➦

1. The collection, processing and use of personal data shall be lawful only if this Act or another legal provision permits or prescribes them or if the data subject has consented.

2. Personal data shall be collected from the data subject. They may be collected without his involvement only if

    1. a statutory provision so provides or requires or

    2. a. the administrative task to be fulfilled by its nature or purpose makes collection from other persons or bodies necessary or

       b. collection from the data subject would entail disproportionate effort

    and there are no grounds for believing that overriding legitimate interests of the data subject would be prejudiced.

3. If personal data are collected from the data subject he shall be informed by the data controller, unless he has already received the information by some other means, of

    1. the identity of the data controller,

    2. the purposes of the collection, processing or use and

    3. the categories of recipients only where in the particular circumstances the data subject cannot be assumed to know of such disclosure.

    If personal data are collected from a data subject on the basis of a statutory provision which requires the information to be furnished or if the furnishing of the information is a prerequisite for obtaining some benefit under the law, then the data subject shall be so advised or, if that is not the case, he shall be advised that provision of data is voluntary. Where necessary in the circumstances of the particular case or at his request he shall be informed of the statutory provision and of the consequences of refusing to provide the data.

Section 4a. Consent ➦

1. Consent shall be effective only if it is based on a free decision of the data subject. The data subject shall be advised of the intended purpose of collection, processing or use and, where the particular circumstances so require or at his request, of the consequences of refusing consent. Consent shall be given in writing except where

special circumstances render some other form appropriate. If consent is to be given in writing simultaneously with other declarations, special prominence shall be given to the declaration of consent

2. In the field of scientific research, special circumstances for the purposes of the third sentence of paragraph (1) above shall include where the requirement of writing would seriously prejudice the purpose of the research. In that event, the advice referred to in the second sentence of paragraph (1) and the reasons for which the purpose of the research would be seriously prejudiced shall be set down in writing.

3. Where special categories of personal data (§ 3, paragraph (9)) are collected, processed or used, the consent shall expressly include a reference to these data.

Section 4b. Transfer of personal data abroad and to supranational and inter-state bodies ➦

1. The transfer of personal data to bodies

    1. in other Member States of the European Union,
    2. in other contracting states to the Agreement on the European Economic Area or
    3. within the institutions and services of the European Communities

    shall be governed by § 15, paragraph (1), § 16, paragraph (1) and §§ 28 to 30 in accordance with the laws and agreements applicable to such transfer, provided the transfer takes place in connection with activities which fall wholly or partly within the scope of the law of the European Communities.

2. The transfer of personal data to the bodies referred to in paragraph (1), which does not take place in connection with activities which fall wholly or partly within the scope of the law of the European Communities, and to other foreign or supranational or inter-state bodies shall be governed by paragraph (1) mutatis mutandi. No transfer shall take place where the data subject has a legitimate interest in opposing transfer, especially where the bodies referred to in paragraph (1) do not offer an adequate level of data protection. The previous sentence shall not apply where the transfer is necessary for the discharge of a Federal public body's own duties on urgent grounds of security or for the performance of multilateral or bilateral obligations in the area of crisis management or conflict prevention or for humanitarian measures.

3. The adequacy of the level of protection shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration can be given to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination, the rules of law, applicable to the recipient and the professional rules and security measures applicable to him.

4. In the cases referred to in the second subparagraph of § 16, paragraph (1), the transferring body shall notify the data subject of the fact that his data have been transferred. The foregoing shall not apply if it can be expected that the data subject will obtain the information by some other means or if the notification would endanger public security or would otherwise be prejudicial to the Federal Republic or to a Land.

5. Responsibility for the lawfulness of a transfer shall be borne by the transferring body.

6. The body to which the data are transferred shall be notified of the purpose for which the data are being transferred.

Section 4c. Exceptions ➦

1. In connection with activities which fall wholly or partly within the scope of the law of the European Communities, the transfer of personal data to bodies other than those referred to in § 4b, paragraph (1), shall be lawful, even where the level of data protection offered is not adequate, if

    1. the data subject has given his consent,

    2. the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures which have been arranged at the data subject's behest,

    3. the transfer is necessary for the formation or performance of a contract which has been or is to be entered into in the data subject's interest by the data controller with 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 vital interests of the data subject or

    6. the transfer is made from a register which is intended to provide information to the public and is open to inspection either by the public in general or by all those who can demonstrate a legitimate interest, provided that the conditions laid down by law are met in the particular case.

    The body to whom the data are transferred shall be advised that the data transferred may be processed or used only for the purpose for which they were transferred.

2. Without prejudice to the first sentence of paragraph (1), the competent supervisory authority may authorize individual transfer operations or particular sets of transfer operations whereby personal data are transferred to bodies other than those referred to in § 4b, paragraph (1), if the data controller shows adequate safeguards with respect to the protection of privacy and the exercise of the associated rights; the safeguards may consist in particular of contract clauses or binding rules of an enterprise. In the case of post and telecommunications organizations, the Federal Data Protection Commissioner shall be competent. Where the transfer is to be made by public bodies, these bodies shall assess whether the conditions described in the first sentence of this paragraph are satisfied.

3. The Länder shall notify the Federal Government of decisions taken pursuant to the first sentence of paragraph (2).

Section 4d. Obligation of registration ➦

1. Before an automated processing operation is put into service it shall be registered in accordance with § 4e, in the case of a non-public data controller, with the competent supervisory authority and, in the case of a public data controller or a post and telecommunications organization, with the Federal Data Protection Commissioner.

2. The obligation of registration shall not apply where the data controller has appointed a data protection officer.

3. The obligation of registration shall further not apply where the data controller collects, processes or uses personal data for its own purposes and employs no more than four staff on the collection, processing or use of personal data and either the consent of the data subject has been obtained or the collection, processing or use furthers the object of a contractual relationship or a quasi-contractual relationship of trust with the data subject.

4. Paragraphs (2) and (3) shall not apply in the case of automated processing operations in which personal data are recorded in the course of business by the body concerned

    1. for the purposes of disclosure or

    2. for the purposes of anonymized disclosure.

5. Where automated processing operations pose particular risks for the rights and liberties of the data subjects they shall be subject to appraisal prior to commencement of processing (prior checking). Prior checking shall be carried out in particular where

    1. special categories of personal data (§ 3, paragraph (9)) are processed or

    2. the purpose of the processing of personal data is to evaluate the data subject's personality including his abilities, his performance or his behavior,

    unless a legal obligation applies or the data subject's consent has been obtained or the collection, processing or use furthers the object of a contractual relationship or a quasi-contractual relationship of trust with the data subject.

6. Responsibility for prior checking shall lie with the data protection officer. He shall carry out the prior checking upon receipt of the particulars referred to in the first sentence of § 4g, paragraph (2). In case of doubt, he shall refer to the supervisory authority or, in the case of the post and telecommunications organizations, to the Federal Data Protection Commissioner.

Section 4e. Particulars required to be notified ➦

Where automated processing operations are required to be notified, the following particulars shall be submitted:

1. the name of the data controller,

2. the proprietors, directors, managers or other persons in charge either by statute or

under the organization's constitution and the persons in charge of data processing,

3. the address of the data controller,
4. the purposes of the data collection, processing or use
5. a description of the categories of data subject and the data or categories of data concerned,
6. recipients or categories of recipient to whom the data can be disclosed,
7. time limits for erasure of the data,
8. any planned transfer of data to third countries,
9. a general description which enables a provisional assessment to be made as to whether the measures under § 9 to safeguard the security of processing are adequate.

§ 4d, paragraphs (1) and (4) shall apply to the modification of the particulars submitted under the first sentence and to the date of commencement and cessation of the activity subject to the notification requirement.

Section4f. Data protection officer ➦

1. Public and non-public bodies which collect, process or use personal data by automated means shall appoint in writing a data protection officer. Non-public bodies shall be bound to do so not later than one month after commencing operations. The same shall apply where personal data are collected, processed or used by some other means and where at least 20 staff are normally employed for that purpose. The first two sentences hereof shall not apply for non-public bodies which employ not more than four staff on the collection, processing or use of personal data. Where necessary because of the structure of a public body, it shall suffice for a single data protection officer to be appointed for several departments. Non-public bodies which perform automated processing subject to prior checking or which collect, process or use personal data in the course of business for the purpose of disclosure or anonymized disclosure shall be required to appoint a data protection officer irrespective of the numbers of staff employed.
2. Eligibility for appointment as data protection officer shall be restricted to those who possess the expertise and reliability necessary for the duties in question. An individual from outside the data controller may be entrusted with the office. Public bodies may, with the approval of their supervisory authority, appoint a civil servant from another public body as data protection officer.
3. The data protection officer shall report directly to the head of the public or non-public body. He shall be independent in the exercise of his professional judgement in the area of data protection. He may not be exposed to any detriment in respect of the performance of his duties. An appointment as data protection officer may be revoked in application of § 626 of the Civil Code or, alternatively, in the case of non-public bodies, at the request of the supervisory authority.
4.

The data protection officer shall be bound to secrecy regarding the identity of the data subject and any circumstances from which the data subject's identity could be inferred, unless released from this obligation by the data subject.

5. The public and non-public bodies concerned shall assist the data protection officer in the performance of his duties and, in particular, shall provide him with staff, premises, facilities, equipment and resources to the extent necessary for the performance of his duties. Data subjects may bring a matter to the attention of the data protection officer at any time.

Section 4g. 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, the data protection officer may apply, in cases of doubt, to the authority in charge of supervising data protection in the data controller. 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 plans for the 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 particular data protection requirements relevant to each case.

2. The data protection officer shall receive from the data controller a statement of the particulars specified in the first sentence of § 4e and of persons having authorized access. Where § 4d, paragraph (2), applies, the data protection officer shall make available in an appropriate manner the particulars specified in the first sentence of § 4e at the request of any party. Where § 4d, paragraph (3) applies, the previous sentence shall apply mutatis mutandi to the data controller.

3. The second sentence of paragraph (2) above shall not apply to the authorities referred to in the fourth sentence of § 6, paragraph (2). The second sentence of paragraph (1) shall apply with the proviso that the administration's data protection officer shall make contact with the head of the authority; in the event of disagreement between the administrative data protection officer and the head of the authority the supreme federal authority shall adjudicate.

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. 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 recorded by automated means such that several bodies are entitled to store and if the data subject is unable to ascertain which body has recorded 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 recorded the data. The data subject shall be informed of that and of the controller's identity. 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 6a. Automated individual decisions ➦

1. Decisions which produce a legal effect for the data subject or which significantly affect him may not be based solely on automated processing of personal data intended to evaluate certain personal features.

2. The foregoing shall not apply if

    1. the decision is taken in the course of the entering into or performance of a contract or other legal relationship and the data subject's request has been satisfied or

    2. the data subject's legitimate interests are protected by suitable measures and the data subject is notified by the data controller of the fact that a decision within the meaning of paragraph (1) has been taken. Suitable measures shall include inter alia arrangements allowing the data subject to put his point of view. The data controller shall be bound to review its decision in that light.

3. The data subject's right to information under §§ 19 and 34 shall extend to knowledge of the logic involved in any automatic processing of data concerning him.

Section 6b. Surveillance of publicly accessible spaces using opto-electronic equipment ➦

1. The surveillance of publicly accessible spaces using opto-electronic equipment (video surveillance) shall be lawful only if it is necessary

    1. for public bodies to discharge their duties,

    2. for exercising control over a premises or

    3. to protect legitimate interests for specifically stated purposes

    and there are no grounds for believing that there are overriding legitimate interests of the data subjects at stake.

2. Notice of the fact that surveillance is taking place and the identity of the data controller shall be given by suitable means.

3. The processing or use of data collected in accordance with paragraph (1) shall be lawful if it is necessary for the attainment of the object pursued and if there are no grounds for believing that there are overriding legitimate interests of the data subjects at stake. The data may be processed or used for some other purpose only where necessary to counter threats to national and public security or for the investigation of crime.

4. If data collected by video surveillance are matched to a particular individual, the individual in question shall be notified of the processing or use in accordance with §§ 19a and 33.

5. The data shall be erased immediately when they are no longer necessary for the attainment of the purpose or where their further retention would be contrary to data subjects' legitimate interests.

Section 6c. Mobile personal data-processing systems ➦

1. A body which supplies a mobile personal data recording and processing medium or which installs on such a medium, modifies or makes available a procedure for the automated processing of personal data which runs wholly or partly on such a medium shall inform the data subject, unless he already has knowledge thereof, of

    1. its identity and address,

    2. the mode of operation of the medium and the nature of the personal data to be processed, expressed in plain language,

    3. how his rights under §§ 19, 20, 34 and 35 may be exercised, and

    4. the steps to be taken in case of loss or destruction of the medium.

2. The body referred to in paragraph (1) shall ensure that the devices or equipment necessary to exercise the right of information are available in sufficient quantities for use free of charge.

3. Communication processes which trigger a data-processing operation on the medium must be clearly identifiable as such to the data subject.

Section 7. Compensation ➦

If a data controller causes loss or damage to the data subject by collecting, processing or using his personal data incorrectly or unlawfully contrary to the provisions of this Act or other data protection provisions, the data controller or the institution to which it belongs shall be liable to pay compensation to the data subject. The obligation to pay compensation shall not apply if the data controller has observed the standard of care appropriate in the circumstances.

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

1. If a data controller causes loss or damage to the data subject by collecting, processing or using his personal data by automated means incorrectly or unlawfully contrary to the provisions of this Act or other data protection provisions, the institution to which it belongs shall be liable to pay compensation to the data subject irrespective of fault.

2. In the case of serious breach of his privacy the data subject shall also be entitled to recover fair compensation in money in respect of damage of a non-financial nature.

3. Claims under paragraphs (1) and (2) above shall be limited to a total amount of DEM 250,000. If as a result of the same event compensation is payable to several persons and the total amount exceeds DEM 250,000, the individual compensation payments shall be reduced pro rata the ratio of the total to that limit.

4. If in the case of an automated processing operation several bodies are authorized to hold record data and if the injured party is unable to determine which body actually recorded the data, each of the bodies in question shall be liable.

5. The issue of contributory fault on the part of the data subject and the issue of limitation shall be governed by §§ 254 and 852 of the Civil Code.

Section 9. Technical and organizational measures ➦

Public and private bodies collecting, processing or using 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 ➦

With a view to improving data protection and data security, suppliers of data-processing systems and programs and data-processing bodies may have their data protection plans and their technical facilities audited and evaluated by independent and licensed experts and publish the results. The detailed requirements applicable to the audit and evaluation, the procedure and the selection and licensing of experts will be laid down in a separate enactment.

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 data are disclosed,

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 Ministry responsible for the controller and for the retrieving body has given its consent.

4. Responsibility for the admissibility of retrieval in a particular case shall rest with the third parties to whom data are disclosed. 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) shall not apply to the retrieval of data which are generally accessible. Data are generally accessible if any person may use them either without or after prior registration, authorization or payment of a fee.

Section 11. Collection, processing or use of personal data by an agent

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. The commission shall be given in writing, specifying the data collection, 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. The principal must satisfy himself that the agent's technical and organizational measures are complied with.

3. The agent may collect, 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 collect, process or use personal data in the normal course of business as service enterprises, sections 4f, 4g and 38 of this Act.

5. Paragraphs (1) to (4) shall apply mutatis mutandi where the testing or maintenance of automated procedures or data-processing systems is carried out by other bodies and the possibility of personal data being accessed cannot be ruled out.

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 to 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 previous, current or future employment-related purposes then instead of §§ 13 to 16, 19 to 20, §28, paragraph (1) and paragraph (3), first subparagraph, as well as §§ 33 - 35 shall apply, even in cases where personal data are neither processed by automated means nor processed or used in non-automated filing systems or collected for that purpose.

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 data controller.

   (1a) If personal data are collected from a non-public body instead of from the data

subject, that body shall be advised of the legal provision under which it is required to make disclosure or else of the fact that disclosure is voluntary.

2. The collection of special categories of personal data (§ 3, paragraph (9)) shall be lawful only if

   1. provided for under law or is urgently needed to protect an important public interest,
   2. the data subject has given consent in accordance with § 4a, paragraph (3),
   3. it is necessary in order to safeguard vital interests of the data subject or of a third party where the data subject is physically or legally incapable of giving his consent,
   4. the data in question have manifestly been placed in the public domain by the data subject,
   5. it is necessary in order to avert a serious threat to public security,
   6. it is urgently necessary in order to avert serious prejudice to the public interest or to safeguard important public interest concerns,
   7. it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional or by another person subject to an equivalent obligation of secrecy,
   8. it is necessary for scientific research purposes and the scientific interest in carrying out the research project substantially outweighs the data subject's interest in opposing collection and the purpose of the research could not be achieved by other means without unreasonable effort or at all, or
   9. it is necessary on compelling grounds relating to defence or the fulfilment of multilateral or bilateral obligations of the Federal Government in the area of crisis management or conflict prevention or for humanitarian measures.

Section 14. Recording, 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 data controller 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 are generally accessible or data controller 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 threat to public safety, or to safeguard important public interest concerns,

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 data controller. This shall also apply to processing or use for training and examination purposes by the data 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 collection, modification or use of special categories of personal data (§ 3, paragraph (9)) for other purposes is lawful only if

1. the conditions under which collection would be lawful as laid down in subparagraphs 1 to 6 or 9 of § 13, paragraph (2) are satisfied or

2. it is necessary for scientific research purposes and the public interest in carrying out the research project substantially outweighs the data subject's interest in opposing the change of purpose and the purpose of the research could not be achieved by other means without unreasonable expenditure or at all.

For the purposes of the determination to be made under subparagraph 2, the scientific interest in the research project shall be given particular consideration in assessing the public interest.

6. The recording, modification or use of special categories of personal data (§ 3, paragraph (9)) for the purposes specified in § 13, paragraph (2), subparagraph 7 shall

be in accordance with the secrecy obligations by which the persons referred to in § 13, paragraph (2), subparagraph 7 are bound.

Section 15. Disclosure 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 third party to whom data are disclosed 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 third party to whom data are disclosed, 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 third party to whom data are disclosed 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 them.

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 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. Disclosure of data to non-public 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 third party to whom data are disclosed 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. Notwithstanding the foregoing, the disclosure of special categories of personal data (§ 3, paragraph (9)) shall be lawful only if the conditions for use under § 14, paragraphs (5) and

(6) are satisfied or if it is necessary for the establishment, exercise or defense of legal claims.

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 third party to whom the data were disclosed 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 him. 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. (Repealed)

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.

2. The public bodies shall keep a register of the data-processing systems employed. For their automated processing operations they shall make a record of the particulars specified in § 4e and the legal basis for the processing. This may be dispensed with in the case of automated processing operations for general administrative purposes in which the data subject's right of information is not restricted pursuant to § 19, paragraph (3) or (4). For automated processing operations which are carried out several times in an identical or similar manner, a composite statement shall suffice.

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 disclosed, 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 in neither automated 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 data controller 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 and disclosure would entail disproportionate effort.

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 data 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 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 data 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 shall be notified of the fact of the recording, the identity of the data controller and the purpose of the collection, processing or use. The data subject shall also be notified of the recipients or categories of recipients of data, unless he must be aware that the data will be disclosed to them. Where a disclosure is envisaged, the notification must take place no later than by the first such disclosure.

2. There shall be no obligation of notification if

    1. the data subject has obtained knowledge by other means of the recording or disclosure,

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

    3. there is express statutory provision for the recording or disclosure of the personal data.

    The data controller shall record in writing the reasons why notification is not given on the basis of subparagraphs 2 or 3 above.

3. § 19, paragraphs (2) to (4), shall apply mutatis mutandi.

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

1. Incorrect personal data shall be corrected. If it is ascertained that personal data which are neither processed by automated means nor recorded in non-automated filing systems are incorrect or if the data subject disputes that they are correct, a note to this effect shall be recorded by suitable means.

2. Personal data which are neither processed by automated means nor recorded in non-automated filing systems shall be erased if

    1. their storage is inadmissible or

    2. knowledge of them is no longer required by the data controller 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 which are neither processed by automated means nor recorded 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 may not be collected, processed or used for automated processing or processing in non-automated filing systems if the data subject objects to the data controller and it is found upon inquiry that the data subject's legitimate interest by reason of his particular personal situation outweighs the data controller's interest in the said collection, processing or use. The previous sentence shall not apply if the collection, processing or use is required by a mandatory provision of law.

6. Personal data which are neither processed by automated means nor recorded in non-automated filing systems 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.

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 data controller or a third party and

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

8. Where 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 data communication, if this does not require disproportionate effort and legitimate interests of the data subject do not stand in the way.

9. Section 2 (1) to (6), (8) and (9) of the Federal Archives Act shall apply.

Section 21. Recourse to the Federal Data Protection Commissioner ➦

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 Data Protection Commissioner ➦

Section 22. Election of the Federal Data Protection Commissioner ➦

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 wellbeing 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 Ministry of the Interior. He shall be subject to the hierarchical supervision of the Federal Ministry 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 Ministry 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 Ministry 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 Data Protection Commissioner ➦

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 board 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. The Federal Commissioner and his staff shall not be subject to §§ 93, 97, 105(1), 111(5) in conjunction with 105(1) and 116(1) of the Abgabenordnung (Tax Code). The fifth sentence hereof shall not apply if the revenue authorities require disclosure for the conduct of proceedings in respect of a criminal offense against the tax laws or proceedings pending in connection therewith, the prosecution of which represents a matter of compelling public interest or in a case of willfully false information given by the person concerned or by others acting for him. If the Federal Commissioner finds a breach of data privacy has been committed, he shall have authority to formally report it and to notify 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. § 28 of the Federal Constitutional Court Act is not affected.

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.

8. Sentences 5 to 7 of paragraph (5) shall apply mutatis mutandi to the public bodies which are responsible for monitoring compliance with the data protection provisions in the Länder.

Section 24. Monitoring by the Federal Data Protection Commissioner ➦

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.

2. The supervisory function of the Federal Commissioner shall also encompass:

    1. personal data acquired by federal public bodies concerning the content and detailed circumstances of letter, postal and telephone communications, and

    2. personal data subject to professional or special official secrecy, in particular tax secrecy under § 30 of the Tax Code.

    The fundamental right to the confidentiality of letter, postal and telephone communications enshrined in Article 10 of the Basic Law is limited accordingly. Personal data subject to supervision by the Commission under § 9 of the Act regulating Article 10 of the Basic Law shall not be subject to the supervision of the Federal Commissioner unless the Commission requests the Federal Commissioner to monitor compliance with the data protection provisions in relation to particular matters or in particular fields and to report the results to it alone. Personal data in records concerning security inspection shall also not be subject to monitoring by the Federal Commissioner if the data subject objects in a particular case to the monitoring of the data concerning him to the Federal Commissioner.

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, 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 Data Protection Commissioner ➦

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,
    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 Data Protection Commissioner ➦

1. The Federal Commissioner for Data Protection shall submit an activity report to the Bundestag every two years. He shall report significant developments in data protection to the Bundestag (lower house of federal parliament) and to the public.

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. The third and fourth sentences of § 38, paragraph (1) shall apply mutatis mutandi.

Part III. Data processing by private bodies and commercial public enterprises ➦

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 are processed or used with the application of data-processing systems or collected for that purpose or the data are processed or used in or from non-automated filing systems or collected for that purpose 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.

    This paragraph shall not apply if the collection, processing or use of the data is carried out solely for personal or domestic activities

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 obtained from automated processing.

Section 28. Collection, processing and use of data for one's own purposes ➦

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

    1. for 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 data controller 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, or

    3. if the data are generally accessible or if the data controller can lawfully publish them, unless the data subject's legitimate interest in precluding processing or use clearly outweighs the justified interest of the data controller.

    In the collection of personal data the purposes for which the data are to be processed or used shall be recorded specifically.

2. They may be disclosed or used for a different purpose only subject to the conditions set forth in subparagraphs 2 and 3 of the first sentence of paragraph (1).

3. Disclosure or use for another purpose shall also be lawful:

    1. where it is necessary to protect the legitimate interests of a third party or

    2. where it is necessary to avert threats to national or public security or for the investigation of crime, or

    3. for purposes of marketing, market research and opinion polling, in relation to data in list form or otherwise combined data on members of a category of persons and restricted to

        a. whether or not the data subject belongs to that category of persons,

        b. occupation, trade or business,

        c. name,

        d. title,

        e. academic degrees

        f. address and

        g. year of birth

    and there are no grounds for believing that the data subject has a legitimate

interest in precluding the disclosure or use or

4. it is necessary in the interest of a research institution for carrying out scientific research and the scientific interest in carrying out the research project substantially outweighs the data subject's interest in precluding the change of purpose and the object of the research could not be achieved by other means without unreasonable effort or at all.

In the cases covered by subparagraph 3, there shall be a presumption that such an interest exists where in accordance with the stated object of a contractual agreement or a quasi-contractual relationship of trust, stored data are disclosed relating to

1. criminal offences,
2. administrative offences and
3. in the case of disclosure by an employer, relating to employment relationships.

4. If the data subject objects vis-à-vis the data controller 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. Upon being approached for the purposes of marketing or market research or opinion polling, the data subject shall be informed of the identity of the data controller and of his right of objection referred to in the previous sentence; if the party making the approach is using data which are held by a body unknown to him, that party shall also ensure that the data subject can find out the origin of the data. Where the data subject objects vis-à-vis the third party to whom the data are disclosed under paragraph (3) above to processing or use for purposes of advertising or of market or opinion research, the recipient shall block the data for such purposes.

5. The third party to whom the data were disclosed may process or use them only for the purpose for which they were communicated to him. Processing or use for other purposes by non-public bodies shall be admissible only if the requirements of paragraphs (2) and (3) above are met; and by public bodies only subject to the requirements of § 14, paragraph (2). The communicating body shall point this out to him.

6. The collection, processing or use of special categories of personal data (§ 3, paragraph (9)) for a party's own business purposes shall be lawful, where the data subject has not given consent in accordance with § 4a, paragraph (3), if

1. it is necessary in order to safeguard vital interests of the data subject or of a third party where the data subject is physically or legally incapable of giving his consent,
2. the data in question has manifestly been placed in the public domain by the data subject,
3. it is necessary for the establishment, exercise or defense of legal claims and there are no grounds for believing that the data subject has an overriding legitimate interest in excluding the collection, processing or use, or

4. it is necessary for conducting scientific research and the scientific interest in carrying out the research project substantially outweighs the data subject's interest in precluding collection and the purpose of the research could not be achieved by other means without unreasonable effort or at all.

7. The collection of special categories of personal data (§ 3, paragraph (9)) shall also be lawful if necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional or by another person subject to an equivalent obligation of secrecy. The processing and use of data for the purposes specified in the previous sentence shall be in accordance with the secrecy obligations by which the persons referred to in the previous sentence are bound. If for a purpose specified in the first sentence hereof data on the health of individuals are collected, processed or used by members of a profession not referred to in § 203, paragraphs (1) and (3) of the Penal Code involving the diagnosis, curing or alleviation of diseases or the manufacture or distribution of medicines, this shall be lawful only subject to the conditions under it would be lawful for a doctor.

8. The special categories of personal data (§ 3, paragraph (9)) may be disclosed or used for another purpose only subject to the conditions set out in paragraph (6), subparagraphs 1 to 4, or the first sentence of paragraph (7). Disclosure or use shall also be lawful if it is necessary to avert substantial threats to national or public security or for the investigation of major crime.

9. Organizations of a non-profit nature with a political, philosophical, religious or trade-union aim may collect, process use special categories of personal data (§ 3, paragraph (9)) if it is necessary for the organization's activity. The foregoing applies only to the personal data of their members or of persons who have regular contact with them in connection with their purposes. The disclosure of these personal data to individuals or bodies outside the organization shall be lawful only subject to the conditions of § 4a, paragraph (3). Paragraph (3), subparagraph 2 shall apply mutatis mutandi.

Section 29. Collection and recording of data in the course of business with a view to disclosure ➦

1. The collection, storage or modification of personal data in the normal course of business for the purpose of communication, in particular if this is for purposes of marketing, information services, commercial address lists or market research and opinion polling, 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 collection, storage or modification or

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

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

2. Communication in connection with the purposes referred to in paragraph (1) shall be

admissible if

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

   b. the data pursuant to section 28 (3), subparagraph 3 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 (3) 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 third party to whom the data are disclosed.

3. The recording of personal data in electronic or printed directories of addresses, telephone numbers, businesses and the like must not take place if the data subject's wishes to the contrary are apparent from the electronic or printed directory or register on which they are based. The recipient of the data must ensure that annotations from electronic or printed directories or registers are included when being incorporated into directories or registers.

4. Section 28 (4) and (5) of this Act shall apply to the processing or use of communicated data.

5. § 28, paragraphs (8) to (9) shall apply mutatis mutandi.

Section 30. Collection and keeping of data in the course of business with a view to disclosure in anonymized form ➦

1. If personal data are collected and stored in the normal course of business in order to communicate 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 data being excluded from modification or

   2. the data can be taken from generally accessible sources or the data controller 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. § 29 shall not apply.

5. § 28, paragraphs (6) to (9) shall apply mutatis mutandi.

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. (Repealed)

Chapter II. Rights of the data subject

Section 33. Notification of the data subject

1. If personal data are recorded for the first time for one's own purposes without the data subject's knowledge, the data subject shall be notified of the recording, the type of data, the purpose of collection, processing or use and the identity of the data controller. If personal data are stored in the normal course of business for the purpose of communication without the data subject's knowledge, the data subject shall be notified of their initial communication and of the type of data communicated. In the cases dealt with in the two previous sentences, the data subject shall also be notified of the categories of recipients where he cannot, in the particular circumstances, be expected to be aware that the data are to be disclosed to them.

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 and notification would entail a 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 recording or disclosure is expressly provided for by law,

    5. the recording or disclosure is necessary for purposes of scientific research and notification would entail a disproportionate effort

    6. the relevant public body has stated to the data controller 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 would entail a disproportionate effort due to the numbers involved, or

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

8. the data are recorded in the course of a business for the purpose of disclosure and

   a. are taken from generally accessible sources, where they relate to those persons who published these data or

   b. the data are compiled in lists or otherwise combined (§ 29, paragraph (2), subparagraph 1 b))

   and notification would entail a disproportionate effort due to the numbers involved.

   The data controller shall set down in writing under what conditions notification can be dispensed with under subparagraphs 2 to 7 above.

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 the origin of these data,

   2. recipients of categories of recipients to whom data are disclosed, and

   3. the purpose of storage.

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 neither stored by automated processing nor in an automated filing system. The data subject may request information on their origin and recipient unless there is an overriding interest in preserving business secrecy.

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), subparagraphs 2, 3 and 5 to 7, 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. the data concerns racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual life, criminal or administrative offences and the data controller 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 course of business for the purpose of disclosure and a review at the end of the fourth calendar year after their first being recorded shows that their further retention 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 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. Personal data may not be collected, processed or used for automated processing or

processing in non-automated filing systems if the data subject objects to the data controller and it is found upon inquiry that the data subject's legitimate interest by reason of his particular personal situation outweighs the data controller's interest in the collection, processing or use. The previous sentence shall not apply if the collection, processing or use is required by a mandatory provision of law.

6. 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 counterstatement.

7. If this does not require disproportionate effort and legitimate interests of the data subject do not stand in the way, 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 data communication.

8. 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 data controller 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. Supervisory authority ➦

Section 36 Repealed ➦

Section 37 Repealed ➦

Section 38. Supervisory authority ➦

1. The supervisory authority shall monitor the application of this Act and of other data protection provisions which regulate the automated processing of personal data or the processing of use of personal data in or from non-automated filing systems including the laws of the Member States in the cases referred to in § 1, paragraph 5. The supervisory authority may process and use the data it holds only for supervisory purposes; § 14, paragraph (2), subparagraphs 1 to 3, 6 and 7 shall apply mutatis mutandi. In particular, the supervisory authority may disclose data to other supervisory authorities for supervisory purposes. It shall provide the supervisory authorities of other Member States of the European Union with supplementary assistance (administrative assistance) on request. If the supervisory authority establishes a breach of this Act or other data protection provisions, it shall have authority to notify the data subject accordingly, report the breach to the bodies responsible for investigating or punishing offences and, in the case of serious breaches, notifying the trade supervisory body (Gewerbaufsichtsbehörde) with a view to the enforcement of trade regulations. It shall publish regularly, not less than every two years, a report of

its activities. The first sentence of § 21 and the fourth to seventh sentences of § 23, paragraph (5) shall apply mutatis mutandi.

2. The supervisory authority shall keep a register of the automated processing operations which are registrable under § 4d, containing the particulars set out in the first sentence of § 4e. The register shall be open to inspection by any person. The right of inspection shall not extend to the particulars referred to in § 4e, subparagraph (9) or to the identity of the persons having access authorization.

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 § 4g. paragraph (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 data protection under this Act and other data protection provisions governing the automated processing of personal data or the processing of personal data in or from non-automated filing systems, 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.

Section 38a. Codes of conduct to promote the implementation of data protection provisions ➦

1. Trade associations and other bodies representing other categories of responsible bodies may submit draft codes of practice for promoting the implementation of data protection provisions to the competent supervisory authority

2. The supervisory authority shall ascertain whether the drafts submitted to it are in

accordance with the data protection provisions in force.

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 data controller 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.

Part IV. Special provisions

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 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.
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 shall make provision in their legislation that the collection, processing or use of personal data by enterprises or auxiliary enterprises in the press sector exclusively for their own journalistic-editorial or literary purposes shall be subject to rules corresponding to the provisions of § 5, § 9 and § 38a including a relevant liability provision corresponding to § 7.
2. If journalistic - editorial collection, processing or use of personal data by the 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 the Deutsche Welle, he may request information on the stored personal data on which the reporting was based. Information may be refused, following appraisal of the legitimate interests of the parties concerned, if

   1. the individuals working or having worked as professional journalists on the preparation, production or broadcast of programs can be identified from the data,
   2. the contributor or source of editorial contributions, materials and news can be identified from the data,
   3. disclosure of data obtained by investigative journalism or otherwise would compromise the journalistic remit of the Deutsche Welle to investigate the facts.

4. In all other respects, §§ 5, 7, 9 and 38a of this Act shall apply to the 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 officer of the Deutsche Welle ➦

1. The Deutsche Welle shall 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 directorgeneral; 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 Deutsche Welle every two years, beginning on 1 January 1994. In addition he shall submit special reports pursuant to a decision by an organ of the Deutsche Welle. The data protection officer shall transmit the activity reports to the Federal Commissioner for Data Protection as well.
5. The Deutsche Welle shall make further arrangements for their area of activity in accordance with sections 23 to 26 of this Act. §§ 4f and 4g are not affected.

Part V. Final provisions ➦

Section 43. Administrative offenses ➦

1. An administrative offense is committed by anyone who, whether intentionally or through negligence,

    1. contrary to § 4d, paragraph (1), and, as the case may be, in conjunction with § 4e, second sentence, fails to register or to do so within the prescribed time limit or fails, when registering, to provide the required particulars or to provide correct or complete particulars,

    2. contrary to § 4f, paragraph (1), first or second sentence, and, as the case may be, in conjunction with the third and sixth sentences, fails to appoint a data protection officer either in the prescribed manner or within the prescribed time limit or at all,

    3. contrary to § 28, paragraph (4), second sentence, fails to inform the data subject within the prescribed time limit, or in due form, or at all, or fails to satisfy himself that the data subject has acquired the knowledge otherwise,

    4. contrary to § 28, paragraph (5), second sentence, discloses or uses personal data,

    5. contrary to the third or fourth sentence of § 29, paragraph (2), fails to record the reasons specified therein or the means of credibly presenting them,

    6. contrary to § 29, paragraph (3), first sentence, records personal data in electronic or printed directories of addresses, telephone numbers, businesses and the like,

    7. contrary to § 29, paragraph (3), second sentence, fails to ensure the inclusion of markings,

    8. contrary to § 33, paragraph (1), fails to notify the data subject correctly, or completely, or at all,

    9. contrary to § 35, paragraph (6), third sentence, discloses data without a counter-statement,

    10. contrary to § 38, paragraph (3), first sentence, or paragraph (4), first sentence, fails to provide information or fails to do so correctly, completely or within the prescribed time limit or refuses to permit a measure or

    11. fails to comply with an enforcement notice issued pursuant to § 38 (5), first sentence.

2. An administrative offense is committed by anyone who, whether intentionally or through negligence,

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

    2. without authorization makes available for retrieval by automated processes personal data which are not generally accessible,

3. without authorization retrieves personal data which are not generally accessible or obtains such data for himself or for another from automated processing operations or from non-automated filing systems,

4. by misrepresentation procures the disclosure of personal data which are not generally accessible,

5. contrary to § 16, paragraph (4), first sentence, § 28, paragraph (5), first sentence, and, as the case may be, in conjunction with § 29, paragraph (4), § 39, paragraph (1), first sentence or § 40, paragraph (1), uses the disclosed data for other purposes by passing them on to a third party, or

6. contrary to § 30, paragraph (1), second sentence, combines the features referred to in § 30, paragraph (1), first sentence or, contrary to § 40, paragraph (2), third sentence, the features referred to in § 40, paragraph (2), second sentence, with the individual particulars.

3. An administrative offense under paragraph (1) is punishable by a fine of up to fifty thousand deutschemarks and an administrative offense under paragraph (2) is punishable by a fine of up to five hundred thousand deutschemarks.

Section 44. Criminal offenses ➦

1. It is an offense punishable by up to two years imprisonment or a fine to commit a deliberate act contrary to § 43, paragraph (2), with a view to enriching oneself or another or with a view to harming another.

2. Such acts shall be prosecuted only on foot of a complaint. A complaint may be brought by the data subject, the data controller, the Federal Data Protection Commissioner or the supervisory authority.

Part VI. Transitional provisions. ➦

Section 45. Existing operations ➦

Operations for the collection, processing or use of personal data which are already in being as of 23 May 2001 shall be brought into compliance with the provisions of this Act within three years after that date. Where provisions of this Act fall to apply in legal provisions outside the scope 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, operations for the collection, processing or use of personal data which are already in being as of 23 May 2001 shall be brought into compliance with the provisions of this Act within five years after that date.

Section 46. Continued validity of definitions ➦

1. Where the term "filing system" is used in specific provisions of federal law it shall mean

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).

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

2. Where the term "record" is used in specific provisions of federal law it shall mean any document serving official or administrative purposes which does not fall within the definition of filing system under paragraph (1); this shall include image and sound recording media. It shall not include preliminary drafts and notes that are not intended to form part of a file.
3. Where the term "recipient" is used in specific provisions of federal law it shall mean any person or body other than the data controller. It shall not include the data subject or persons or bodies which collect, process or use personal data on another's behalf in another Member State of the European Union or in another contracting state to the Agreement on the European Economic Area.

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

Where personal data are processed or used by automated means, the internal organization of the authority or the establishment shall be arranged in such a way as to meet the special requirements of data protection. In particular, measures appropriate to the type of personal data to be protected shall be taken

1. to prevent unauthorized persons from gaining entry to data-processing installations where personal data are processed or used (entry control),
2. to prevent the use of data-processing systems by unauthorized persons (access control),
3. to ensure that persons authorized to use a data-processing system can gain access only to the data they have authority to access and that personal data cannot be read, copied, modified or removed without authorization during processing, use or after being recorded (intervention control),
4. to ensure that during electronic disclosure or during transport or storage on data media, personal data cannot be read, copied, modified or removed without authorization and that it is possible to verify and establish to which bodies a disclosure of personal data by means of data disclosure equipment is planned (disclosure control),
5. to ensure that it is possible to verify and establish ex post facto whether and by whom personal data were entered into data-processing systems, modified or removed (input control),
6.

to ensure that personal data being processed by a processing agent can be processed only in accordance with the principal's instructions (agent control),

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

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