

### 3. FEDERAL GERMAN REPUBLIC

#### DATA PROTECTION BILL

Presented to Parliament on  
21 September 1973

#### Part I

#### *General Provisions*

##### SECTION 1

#### *Purpose of the Act*

1. The purpose of this Act is the protection of personal data against misuse by data processing and by that to counteract prejudices of protective interests of the persons concerned. Data protecting comprises all measures which serve to prevent prejudice to any personal interests that warrant protection during the processing of personal data stored in data banks.

##### SECTION 2

#### *Field of application*

(1) This Act shall serve to protect personal data in so far as these are stored in data banks or otherwise processed:

1. by public administrative offices or any other public establishments (para. 5),
2. by persons, companies or other societies based on private law for their own purpose (para. 16),
3. by persons, companies or other societies based on private law for third parties in the normal course of business (para. 13).

If personal data should be passed on to third parties, in deviation from their destination named in sentence 1, the relevant sections of this Act should be applied.

(2) Nothing in this Act shall be construed as protecting personal data which can be directly obtained from generally accessible sources. Furthermore, it does not protect personal data as far as they are stored or passed on for the purpose of publication by ordinary or legal persons, establishments or other associations which are or own enterprises of press, broadcasting or films.

## *Appendix B*

(3) The utilisation of personal data protected by this Act shall only be admissible if:

1. the person concerned has agreed, or
2. this Act or another legal decree has permitted it. Permission has to be written, as far as another form is not required by special circumstances; if the permission is given together with other declarations it must be specifically notified to the person concerned.

### SECTION 3

#### *Definitions*

(1) By 'personal data' (in the meaning of this Act) are meant particulars concerning the personal or material characteristics of an identified or identifiable natural person (hereinafter termed 'the person concerned').

(2) 1. 'Data processing' means in particular the storage, modification, communication and erasure of data.

2. 'Storage' means the fixation of data in a data-carrier for the purpose of further application.

3. 'Modification' means to modify stored data in their contents.

4. 'Communication' means to inform third parties about stored data.

5. 'Erasure' means to make stored data unrecognisable irrespective of the process employed.

(3) A data bank within the meaning of this Act is a collection of data intended for evaluation and for communication to third parties, and processed and sorted according to a pre-arranged system irrespective of the process used. Files, collections of files and books are not parts of a data bank.

### SECTION 4

#### *Technical and organisational measures for the protection of data*

(1) Any person processing personal data in accordance with Section 2 (1) shall take the requisite technical and organisational measures to prevent abuses in the course of such processing, especially wrongful retrieval, communication, modification and erasure of data. Only those measures are required whose protective effects are in reasonable proportion to the cost involved.

(2) The Federal Government shall be empowered, with the consent of the Bundesrat, to issue regulations containing basic principles

governing the measures referred to in Sub-section 1, and on the introduction and implementation of such measures. Such regulations may also contain specific measures in accordance with Sub-section 1 and detailed instructions concerning Section 7 (3), Section 8 (4), Section 9 (2), Section 13, sentence 2, Section 18, sentence 4, Section 19, sentence 3, Section 24 (2), sentence 4, Section 25, sentence 3, Section 28, sentence 2, Section 29, sentence 2. The Federal Government with the consent of the Bundesrat, may delegate the powers conferred by sentence 2 of this Sub-section to the Land Governments by means of a governmental decree.

## Part II

*Data processing by governmental administrative departments and other public offices*

### SECTION 5

[Field of application – public sector]

### SECTION 6

*Data storage*

The storage of personal data shall be permitted as part of the legitimate fulfilment of the tasks for which the storage unit is responsible.

### SECTION 7

*Exchange of data by public departments*

(1) The transmission of personal data concerning a special professional or official secret and which are transmitted to the transmitting office by the person who is obliged to observe secrecy in execution of his professional or official duty, shall be permissible if the recipient needs them in order to achieve the fulfilment of the same duties for which the transmitting office received them. The transmission of other personal data shall be permissible in the framework of legitimate fulfilment of tasks for which the recipient is competent.

(2) It is permitted to transmit personal data to public-law religious committees in so far as adequate measures for the protection of such data have been taken by the recipient.

(3) In cases where personal data may be communicated by automatic devices, steps shall be taken to ensure that this happens only

## Appendix B

within the admissible limits and in particular that no unauthorised person can obtain such data.

(4) By documentation of the data programme and if necessary by supporting material, it shall be shown to which public office and to what extent data are communicated. If data are automatically retrieved, a record shall be kept which shows the retrieving office as well as the time and manner of the retrieval.

### SECTION 8

#### *Communication of data to third parties*

(1) Communication of personal data, concerning a special professional or official secret which are transmitted to the transmitting office by the person who is obliged to observe secrecy in execution of his professional or official duty, to parties other than the person concerned or to offices other than those referred to in Section 7 (1) and (2) shall be permissible if equal conditions are given under which the person under obligation of secrecy would be permitted to transmit them.

Communication of other personal data shall be permissible in the framework of legitimate fulfilment of tasks for which the transmitting office is competent or as far as the recipient verified a justifiable interest in knowing the data concerned and by this transmission protectable interests of the person concerned are not violated.

As regards the communication of data to public administrative offices and to any other authorities outside the field of application of this Act and to supranational and international establishments, sentences 1 and 2 shall apply in accordance with the existing laws and agreements regarding such communication.

(2) Exceptions to the terms of Sub-section 1 shall be made in the case of the communication of the following data (unrestricted data):

1. Name
2. Title, academic degrees
3. Date of birth
4. Profession, commercial designation
5. Address
6. Telephone number.

(3) If there is evidence to justify the presumption that a risk to the life, health or personal freedom of the person concerned or any other person may arise as a result of the communication of data, the communication of personal data in the sense of Sub-sections 1 and 2 may not take place.

## *Privacy and Computers*

(4) Section 7 (3) shall apply to the communication of personal data by automatic devices.

### SECTION 9

#### *Modification of data*

(1) The modification of personal data shall be permissible in order to further the legitimate fulfilment of the tasks for which the storage unit is competent. The obligation to correct data under the terms of Section 12 (1) holds good.

(2) In the case of automatic data processing, arrangements shall be made to ensure that data are modified only within the admissible limits.

### SECTION 10

#### *Public notice concerning stored data*

Immediately following the initial act of storage, the storage unit shall announce publicly in the official bulletin what type of personal data are stored by it as well as the category of persons concerned. Sentence 1 shall not apply to offices for the protection of the Constitution, the Federal Intelligence Service, the offices of the Public Prosecutor, the Police Department as well as to the Taxation authorities of the Bund and the Länder as far as they store or use personal data in data banks for controlling and examining them in fulfilling their legitimate tasks in the scope of the Taxation Act of the Reich.

### SECTION 11

#### *Provision of information*

(1) The person concerned shall, upon application, be supplied with information on stored data concerning his own person. The applicant must give details of the type of personal data on which information is sought. The manner and, in particular, the form in which information is supplied shall be left to the discretion of the storage agency.

(2) Sub-section 1 shall not apply to the public authorities referred to in Section 10 (2).

(3) There shall be no obligation to supply information:

1. if the information would be prejudicial to legitimate fulfilment of the tasks for which the storage agency is competent

## *Appendix B*

2. if it would be prejudicial to public security or the public weal of the Federal Republic or of a Land
3. if the personal data or the fact of their storage must be kept in secret following a legal decree or by reason of their character, in particular in view of a preponderant and legitimate interest of a third person
4. if the information concerns the communication of personal data to public authorities referred to in Section 10 (2).

(4) The supply of information shall be subject to the payment of a fee. The Federal Government shall be empowered to determine by decree, with the consent of the Bundesrat, precisely what items shall be liable to the payment of a fee and to specify its amount and any exemptions therefrom. In particular, the fee may be waived in cases where, through special circumstances, it may justifiably be presumed that personal data have been stored inaccurately, confusedly or wrongfully, or where the information supplied has led to the correction, clarification or erasure of personal data in storage. Otherwise the Administrative Fees Act shall apply.

### SECTION 12

#### *Correction and erasure of data*

(1) Personal data shall be corrected when they are incorrect. If the accuracy of personal data is contested by the person concerned, and the alleged inaccuracy cannot be substantiated, an appropriate note shall be included with the data whenever subsequently communicated.

(2) Personal data can be erased when their storage is inadmissible or when they are no longer required by the storage unit for the legitimate fulfilment of the tasks for which it is competent and failure to erase them would harm the legitimate interests of the person concerned; personal data shall be erased when their storage is inadmissible.

(3) Personal data shall be locked when they are no longer required for the fulfilment of the tasks for which the storage unit is competent and if by not locking them protectable interests of a person concerned would be harmed. Locked data shall be signed, they shall not be used further, and in particular, they shall not be communicated, with the exception of use for scientific reasons, for removal in a case of lack of evidence, or by reason of preponderant interest of the storage unit or if the person concerned agrees to their use.

## *Privacy and Computers*

### SECTION 13

#### *Processing of personal data on behalf of other public administrative offices and similar establishments*

The administrative offices and other establishments referred to in Section 5 (3), sentences 2 and 3 shall be permitted to communicate, modify and erase personal data only with the agreement of the administrative offices or other establishments for which the data are stored and processed. In the case of automatic data processing steps shall be taken to ensure that data are communicated, modified and destroyed only within the admissible limits and that they cannot be retrieved by unauthorised persons.

### SECTION 14

#### *Implementation of data protection in the Federal governmental departments*

The highest Federal authorities, the governing body of the German railways and any public-law corporations, institutions and foundations directly responsible to the Federal Government over which legal supervision is solely carried out by some senior Federal authority shall be each and severally required to ensure implementation of this Act and of any other legal provisions on data protection. They shall in particular ensure:

1. that a list is made of the type of personal data held in storage, of the tasks for whose fulfilment a knowledge of the data is required, and of the regular recipients thereof, and
2. that the data processing programmes by means of which personal data are to be processed are checked for orderly application and for conformity with the regulations governing their use.

### SECTION 15

#### *General administrative provisions*

The highest Federal authorities and the governing body of the German railways shall each issue general administrative regulations for their fields of competence which shall govern application of this Act and take account of the circumstances peculiar to each area of activity and any resultant particular requirements concerning data protection.

## Part III

#### *Data processing by non-official establishments for their own purposes*

## Appendix B

### SECTION 16

#### *Field of application*

The provisions of this Part shall apply to natural or legal persons, companies or other groups of private law, in so far as they store in data banks or otherwise process data concerning persons (Section 2 (1)) with whom they have a contractual relationship, or a quasi-contractual relationship of trust, as an aid to the fulfilment of their commercial functions or aims. They shall also apply in the terms of sentence 1, with the exception of Section 22, to commercial insurances under public law and to public-law credit institutions.

### SECTION 17

#### *Data storage*

Storage of personal data is permissible within the framework of the purpose of a contractual relation or quasi-contractual relation of trust with the person concerned or as far as it is required to protect legitimate interests of the storage unit and if there is no reason for the assumption that by this protection-worthy interests of the person concerned will be prejudiced.

### SECTION 18

#### *Communication of data*

Communication of personal data which concern a professional or official secret (Section 37, sentence 2 no. 1, sentence 3), and which are given to the communicating office by the person obligated to keep secrecy, in execution of a professional or official duty, shall be permissible if the requirements are present under which the person obliged to keep secrecy should be allowed to communicate them.

Communication of other personal data is permissible within the framework of the purpose of contractual relations or quasi-contractual relations of trust with the person concerned or as far as it is required to protect legitimate interests of the communicating office or a third party and by that protection-worthy interests of the person concerned are not prejudiced. Communication of free data (Section 8 paragraph 2) is, notwithstanding sentence 1 and 2, always permissible. Section 7, paragraph 3 shall also apply *mutatis mutandis*.

### SECTION 19

#### *Modification of data*

Personal data may be modified only in the context of existing contractual relations or quasi-contractual relations of trust with the



## *Privacy and Computers*

person concerned, or in so far as it is required to protect legitimate interests of the storage unit and by that legitimate interests of the person concerned are not prejudiced.

### SECTION 20

#### *Supply of information*

(1) When personal data on the person concerned are stored for the first time, the person concerned must be informed unless he gets to know of the fact of the storage in another way.

(2) The person concerned may demand information on stored data concerning his person. He shall be required to give details of the type of personal data on which information is sought. Information is to be given in writing unless, in special circumstances, some other form of information is appropriate.

(3) A fee may be required for the information which must not exceed the costs that result directly from supplying it. Sentence 1 shall not apply where the information has led to the correction, clarification or, under the terms of Section 21 (2), second sentence, the erasure of personal data.

(4) Sub-sections 1 and 2 are not applicable as far as:

1. the supply of personal data would seriously impair the functions of the place of storage
2. the supply of personal data would entail a risk to public security or order or to the public weal of the Federal Republic or of any Land
3. the personal data must be kept secret by reason of a decree or by their nature, in particular because of the overriding legitimate interests of a third party.

### SECTION 21

#### *Correction and erasure of data*

(1) Personal data shall be corrected when they are incorrect. Where the accuracy of personal data is contested by the person concerned and the alleged inaccuracy cannot be substantiated, an appropriate note shall be included with the data on the occasion of each subsequent communication.

(2) Personal data may be erased when they are no longer required for the fulfilment of the purpose of the storage and when the erasure is not prejudicial to protection-worthy interests of the person concerned. They shall be erased when their storage is inadmissible.

## *Appendix B*

(3) Personal data shall be locked if they are no longer required for the fulfilment of the purpose of the storage and the person concerned demanded it. The sections concerning the procedure and the legal consequences in Section 12, paragraph 3, sentence 2 shall apply *mutatis mutandis*.

### SECTION 22

#### *Data protection in practice*

(1) Persons, companies and other groups of persons referred to in Section 16 paragraphs 1 and 2 which carry out automatic data processing and give regular employment for at least five permanent staff, shall, at the latest within one month of the commencement of their activity, appoint a data protection officer whose task it will be to ensure that this Act and any other regulation on data protection are properly observed. To that end he shall be directly subordinate to the owner, management, director or any lawfully or constitutionally appointed head of the establishment. Sentence 1 shall also apply to establishments where data processing, though not automatic, provides regular employment for at least twenty permanent staff.

(2) The duties of the data protection officer shall include:

1. Supervision of the type of personal data being stored, of the purposes for which knowledge of such data is required, and of the persons who regularly receive such information,

2. Supervision of the proper application of the data processing programs by means of which personal data are to be processed and and

3. Briefing staff engaged in data processing with regard to the provisions of this Act and any other provisions concerning data protection, with particular reference to the special conditions obtaining in this area of activity and any consequential requirements in the matter of such protection.

## Part IV

### *Routine data processing by non-public establishments on behalf of third parties*

### SECTION 23

#### *Field of application*

The following Sections apply to natural persons, companies or other personal groups of private law:

## *Privacy and Computers*

1. Sections 24 to 27, 30 and 31 of this Part, in so far as the establishments in question store personal data in data banks in the normal course of business for the purpose of communicating them to others and in fact so communicate them; the question of whether the data are modified prior to communication or at any time is of no consequence;

2. Sections 28, 30 and 31, in so far as these establishments store personal data in data banks in the normal course of business for purposes of modification and communication, modify them in such a way that the data neither refer to nor permit recognition of any particular person (render anonymous) and communicate the data in that form;

3. Articles 29 to 31, in so far as these establishments store in data banks and in any way whatsoever modify or process personal data in the normal course of business on behalf of third parties; exceptions shall be made in the case of bodies corporate and associations of persons under private law whose majority of shares or votes is publicly controlled, in so far as such bodies operate on behalf of administrative authorities or other public establishments.

### SECTION 24

#### *Data storage and transmission*

(1) Storage of personal data shall be permitted in so far as there is no reason for the assumption that it will be prejudicial to the protection-worthy interests of the person concerned.

(2) The communication of personal data is permissible only where the applicant gives credible proof that he has a legitimate interest in knowing them. A legitimate interest may arise particularly in connection with a credit, insurance or service contract. The grounds for the existence of legitimate interests and the means of proof adduced shall be recorded. Sections 7 (3) shall apply *mutatis mutandis*.

(3) Notwithstanding the provisions of Sub-section 2, first sentence, communication shall be permissible when limited to unrestricted data (Section 8 (2) ), as far as it is limited to the information concerning the membership of the person concerned to an association of persons and if there is no reason for the assumption that it is prejudicial to the protection-worthy interests of the person concerned.

## *Appendix B*

### SECTION 25

#### *Modification of data*

Modification of personal data is permissible. The obligation to carry out corrections in accordance with Section 27 (1) remains unaffected. Section 9 (2) shall apply *mutatis mutandis* if it is not prejudicial to the protection-worthy interests of the person concerned.

### SECTION 26

#### *Notification*

(1) The person concerned shall be notified whenever data concerning his own person have been communicated. Sentence 1 shall not apply to communication within the terms of Section 24 (3).

(2) The person concerned may demand information concerning stored data relating to his own person. Such information shall be supplied in writing unless some other form of notification is appropriate by reason of particular circumstances.

(3) A fee may be charged for the supply of such information but may not exceed the costs that arise directly from such supply. Sentence 1 shall not apply where the information has led to the correction, clarification or, under the terms of Section 27 (3), second sentence, erasure of personal data.

(4) Sub-sections 1 and 2 shall not apply where knowledge of the personal data may be prejudicial to public security or order or the common weal in the Federation or any Land or to any overriding legitimate interests of a third party.

### SECTION 27

#### *Correction and erasure of data*

1. Personal data shall be corrected when they are incorrect; they are to be clarified when they are unclear. If the accuracy of personal data is contested by the person concerned and the alleged inaccuracy cannot be substantiated a corresponding note shall be added to the data. In the cases referred to in sentence 2 the person concerned may also demand that his dissenting opinion be included in the data.

(2) Any correction, clarification, note or dissenting opinion shall be transmitted to all persons who previously received the data in question. Data to which a note or dissenting opinion have been added may not be communicated without such note or opinion.

## *Privacy and Computers*

(3) Personal data may be erased where the person concerned has no overriding legitimate interests which stand in the way. They shall be erased when their storage is inadmissible.

(4) Personal data shall be locked at the end of the fifth year from the time of their storage if the person concerned so requests.

The rules concerning the procedure and the legal consequences of locking in Section 12 paragraph 3 sentence 2 shall apply *mutatis mutandis*.

### SECTION 28

#### *Processing of personal data for the purposes of communication in anonymous form*

(1) The persons, companies and other groups of persons mentioned in Section 23 paragraphs 1 and 2 are obliged to render anonymous stored personal data when they are no longer required for the purpose of storage; at the latest at the end of the fifth year after storage. Characteristics which could be used in this way that data which has been made anonymous could identify a persons or permit to reveal that person shall be separately stored. These characteristics shall not be stored together with anonymous data except when the use of these locked data is required for the purpose of storage or for scientific reasons.

(2) In the case of automatic data processing, arrangements shall be made to ensure that data are communicated only to the admissible extent and in the admissible form and that they cannot be retrieved by unauthorised persons; the execution of measures mentioned in paragraph 1 shall be ensured by appropriate arrangements.

### SECTION 29

#### *Processing of personal data on behalf of third parties*

(1) The persons, companies and other groups of persons referred to in Section 23 (1), third sentence, shall be allowed to communicate, modify and erase personal data only with the agreement of the persons and establishments on whose behalf the data are stored in data banks or otherwise processed. Arrangements shall be made in the case of automatic data processing to ensure that data are communicated, modified or erased only within the admissible limits and that they cannot be retrieved by unauthorised persons.

## Appendix B

### SECTION 30

#### *Registration*

(1) The persons, companies and other groups of persons referred to in Section 23 (1) and their subsidiary branches and dependent agencies shall be required to register the commencement of their activity with the competent supervisory authority within one month.

(2) The following information on the establishments referred to in Section 23 (1) shall be supplied to the supervisory authority for entry in the register:

1. Name or firm
2. Proprietor of the firm, leading persons
3. Address
4. Purpose of the establishment and of data processing
5. Type and content of programs used in data processing
6. Type of automatic data processing used
7. Type of stored data.

(3) Sub-section 1 shall apply *mutatis mutandis* as regards termination of such activity and as regards any modification of the details supplied in accordance with Sub-section 2.

### SECTION 31

#### *Supervisory authority*

(1) The supervisory authority competent by the law of a Land shall watch over implementation of this Act and any other provisions concerning the protection of data within the field of application of this Part; it shall keep the register of persons, companies and other groups of persons referred to in Section 23 (1); everyone who has a justified interest can examine the register.

(2) Owners of establishments subject to compulsory registration of their activities under Section 31 and persons responsible for the management of such establishments shall be required to supply the supervisory authority with all the information needed for the fulfilment of its tasks. Such owners or other persons may refuse to answer any questions which would expose them or any members of their staff as defined in Article 383 (1) 1 to 3 of the Code of Civil Procedure to the risk of criminal proceedings or proceedings under the Administrative Offences Act.

(3) Persons appointed by the supervisory authority to exercise control over the undertaking concerned shall be empowered, as far as is required for the fulfilment of the duties devolving upon that authority,

to enter the grounds and premises of the enterprise to carry out tests and inspections there and to examine the installation programmes. Owners or other persons responsible for supplying information shall be in duty bound to permit such acts. Fundamental rights of privacy (Article 13 of the basic law) shall be limited to that extent.

(4) Application of the Commercial Code to commercial firms subject to the provisions of this section remain unaffected.

## Part V

### *Penalties and fines*

#### SECTION 32

##### *Penalties*

- (1) Any person or persons who
  1. communicate or change, or
  2. retrieve or procure from a closed holder in a data bank personal data protected by this Act, shall be liable to a term of imprisonment not exceeding one year or to a fine.
- (2) Any person who improperly processes or communicates the personal data either for consideration or with the intention of harming another person or of benefiting himself or another person shall be liable to a term of imprisonment not exceeding two years or to a fine.
- (3) Prosecution shall take place only if a complaint is filed.

#### SECTION 33

##### *Breach of duty of secrecy*

- (1) Any person who improperly discloses a business secret, especially if it was revealed to him as an employee or commissioner of the supervisory authority, shall be liable to a term of imprisonment not exceeding one year or to a fine.
- (2) Any person who acts either for consideration or with the intention of harming another person shall be liable to a term of imprisonment not exceeding two years or to a fine. A person is liable to the same punishment if he improperly uses a secret not belonging to him, especially a business secret, revealed to him under the conditions referred to in paragraph 1.
- (3) Prosecution shall take place only if a complaint is filed.

## *Appendix B*

### SECTION 34

#### *Administrative offences*

(1) An administrative offence shall be deemed committed by any person who, either intentionally or through negligence:

1. contrary to Section 20 (1) in conjunction with Section 16 (1), Section 26 (1), in conjunction with Section 23 (1), fails to notify the person concerned;
2. contrary to Section 22 (1) sentence 1 or 3 fails to appoint an officer responsible for the protection of data or fails to do so within the prescribed time-limit;
3. contrary to Section 24 (2) sentence 3 does not record the grounds named in that section;
4. contrary to Section 26 (1) and (4) fails to notify the person concerned of the initial communication of data relating to his own person;
5. fails to comply with the registration requirements of Section 30 (1) and (3) or fails to do so within the prescribed time-limit;
6. fails to supply the information required under Section 32 or fails to supply accurate and complete details or fails to do so within the prescribed time-limit;
7. contrary to Article 31 (2) and (3) fails to supply information, fails to supply accurate and complete information or fails to do so within the prescribed time-limit, refuses entry into the premises or installations or refuses inspection or examination of records;
8. contravenes the provisions of legal regulations issued on the basis of Section 4 (2), provided that such regulations contain explicit mention of a fine in a particular circumstance.

(2) An administrative offence may be punishable by a fine of up to 50,000 DM.

### Part VI

#### *Transitional and final provisions*

### SECTION 35

[Transitional provisions]

### SECTION 36

[Application of the Administrative Proceedings Act]



*Privacy and Computers*

SECTION 37

[Provisions for the protection of data which continue to apply]

SECTION 38

[Berlin – special clause]

SECTION 39

[Entry into force]