

4. LAND RHINELAND-PALATINATE

(Federal Republic of Germany)

DATA PROTECTION ACT

OF 24 JANUARY 1974

PART I: DATA PROTECTION

Section 1

Subject of data protection

(1) In electronic data processing, especially in the establishment of data banks, by authorities or establishments of the Land as well as by public corporations, institutions and foundations subject to the supervision of the Land, care shall be taken not to disadvantage or injure the interests entitled to protection of natural or legal persons or of associations having no legal status by the collection, storage, use or erasure of data (data protection).

(2) Data protection extends to all data which are subject to an obligation of official confidence or special obligations of secrecy, especially all personal data, regardless of the form of their representation. Only those data are excepted which do not allow the identification of natural or legal persons or associations having no legal status.

Section 2

Manner of data protection

(1) Data to be protected shall be so collected, transferred and stored as not to enable them to be accessed, retrieved, changed or otherwise used by unauthorised persons. This shall be secured by appropriate organisational as well as machine-technical and program-technical safeguards.

(2) The security measures shall be laid down in detail in service instructions.

(3) Where protected data are transferred by autonomous arrangements, every retrieval shall be so recorded as to establish the recipient, content and time of the transfer of data.

Section 3

Data secrecy

(1) Without prejudice to other obligations of secrecy, all persons entrusted with electronic data processing functions in the establishments referred to in Section 1 paragraph (1) are prohibited from communicating protected data to unauthorised persons or from enabling them to acquire knowledge of them or from using such data for a purpose other than one required for the completion of the respective task or from making them accessible to unauthorised establishments or persons.

(2) These persons shall be put under a special obligation to preserve data secrecy when they begin their activities. The obligation of data secrecy continues after the completion of the activities.

Section 4

Regulation of data use

(1) The establishments referred to in Section 1 paragraph (1) may use data subject to data protection, or make them available to others charged with public tasks, only to the extent that this is necessary for the performance of statutory tasks. Data subject to data protection may be made available to other establishments only if and insofar as this is permitted by statute.

(2) The storage of data subject to data protection in data banks and their use in information systems by the establishments referred to in Section 1 paragraph (1) is permitted insofar as it has been ensured that data cannot be accessed, retrieved or otherwise used by unauthorised persons.

(3) Data containing no individual indications about natural or legal persons or about associations having no legal status, and which enable no such individual indications to be inferred, may be transferred and published unless this is precluded by a statutory prohibition or an important public interest.

Section 5

Right of Land Parliament and local representative bodies to information

The Land Parliament, its president, the parliamentary parties

Appendix B

and the representative organs of local authorities may, within the limits of their respective competences, require from the establishments referred to in Section 1 information based on data collected by them, provided that the conditions of Section 4 paragraph (3) are complied with.

PART II: SUPERVISION OF DATA PROTECTION

Section 6

Data Protection Committee

(1) The supervision of data protection is conferred on a Committee, consisting of three members of the Land Parliament and two Land officials or judges. The members of Parliament and one official or judge shall be elected by the Land Parliament to hold office during its electoral life; the second official or judge shall be nominated by the Land Government.

(2) The members of the Committee are independent and free from directions.

(3) [Payment of daily fees and expenses for Committee members]

(4) The Committee shall order its own proceedings.

Section 7

Duties of the Committee

(1) The Committee shall supervise compliance with this Act and other regulations about data protection in electronic data processing by the establishments referred to in Section 1 paragraph (1).

(2) The Committee shall report established infringements to the appropriate supervisory authority and shall recommend safeguards for the improvement of data protection. The supervisory authority shall report to the Committee on what has been achieved on the basis of its findings and recommendations.

(3) [Experts and staff]

Section 8

Duty of secrecy

The members of the Committee and those employed or commissioned by them shall be subject to the duty of secrecy referred to in Section 3 of this Act.

Section 9

Duty to report

With effect from 1 October 1974, the Committee shall submit a report of its activities to the Land Parliament annually on 1 October, dealing particularly with any established infringements of the data protection provisions.

Section 10

Duties of data processing *authorities* and institutions to the Committee.

(1) All the establishments referred to in Section 1 paragraph (1) shall give the Committee the information necessary for the performance of its duties, explain the programs in use, and facilitate the necessary control of security measures.

(2) The establishments referred to in Section 1 paragraph (1) shall report to the Committee the data entitled to data protection to be collected, as well as the manner and extent of their use. The report shall include:

1. a review of data collected,
2. the purpose of use, with reference to all application programs,
3. the group of users, including the programs available for each user,
4. the security measures provided, together with the service instructions instituted for them.

Every change in these indications shall be reported to the Committee within four weeks.

PART III: RIGHTS OF THE DATA SUBJECT

Section 11

Right to information

(1) Everyone has the right to information about data stored relating to himself, so far as this is not excluded by statute, or the data are those of the intelligence service of the Criminal Police or the Office for the Protection of the Constitution.

(2) The information shall be given by a print-out of the stored data. If the data subject has on a previous occasion received a print-out of all the data which relate to him, the information can be restricted to changes and additions after that occasion.

Appendix B

Section 12

Right to correction or erasure

If data entitled to data protection are incorrect or out of date, their subjects may require their correction or erasure. Erasure may be required if the data are no longer necessary for the performance of statutory tasks.

Section 13

Damages

(1) If a data subject is injured in his rights through the unlawful storage, access, change, destruction or retrieval, he can demand compensation unless Federal provisions prevent this. This is without prejudice to additional claims for restitution or compensation based on other legal provisions.

(2) The ordinary courts shall be competent for claims under paragraph (1).

Section 14

Rights of appeal for incorrect storage of data

Everyone shall have the right to appeal to the Data Protection Committee if he is of the opinion that he has been injured in his rights through the collection, storage, or use of data about his personal circumstances by the establishments referred to in Section 1 paragraph (1).

PART IV: FINAL PROVISIONS

Section 15

Penal provisions

(1) Whoever, without authority, reveals data entitled to data protection which have become known to him in connection with automatic data processing, or allows access to such data, shall be punished with deprivation of liberty up to one year or with a fine, or both.

(2) If the act is done for reward or in order to obtain a financial advantage for the actor or for another, or to damage another, the punishment shall be deprivation of liberty up to two years. A fine may be substituted.

(3) A person who, without authority, obtains or uses such data

Privacy and Computers

without belonging to the group of persons referred to in paragraph (1) shall be punished likewise.

(4) The provisions of paragraphs (1) to (3) shall apply only insofar as the act is not visited with higher penalties by other provisions.

(5) The act shall only be prosecuted on the application of the person injured. The prosecution may be withdrawn.

Section 16

[Coming into Force]