**NB: Unofficial translation**

# Personal Data Act

(523/1999)

Chapter 1 — **General provisions**

Section 1 — *Objectives*

The objectives of this Act are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice.

Section 2 — *Scope of application*

(1) The provisions of this Act apply to the processing of personal data, unless otherwise provided elsewhere in the law.

(2) This Act applies to the automatic processing of personal data. It applies also to other processing of personal data where the data constitute or are intended to constitute a personal data file or a part thereof.

(3) This Act does not apply to the processing of personal data by a private individual for purely personal purposes or for comparable ordinary and private purposes.

(4) This Act does not apply to personal data files containing, solely and in unaltered form, data that have been published by the media.

(5) Unless otherwise provided in section 17, only sections 1—4, 32, 39(3), 40(1) and (3), 42, 44(2), 45—47, 48(2), 50, and 51 of this Act apply, where appropriate, to the processing of personal data for purposes of journalism or artistic or literary expression.

Section 3 — *Definitions*

In this Act,

(1) *personal data* means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household;

(2) *processing of personal data* means the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data;

(3) *personal data file* means a set of personal data, connected by a common use and processed fully or partially automatically or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved easily and at reasonable cost;

(4) *controller* means a person, corporation, institution or foundation, or a number of them, for the use of whom a personal data file is set up and who is entitled to determine the use of the file, or who has been designated as a controller by an Act;

(5) *data subject* means the person to whom the personal data pertains;

(6) *third party* means a person, corporation, institution or foundation other than the data subject, the controller, the processor of personal data or someone processing personal data on the behalf of the controller or the processor;

(7) *consent* means any voluntary, detailed and conscious expression of will, whereby the data subject approves the processing of his/her personal data;

(8) *personal credit data* means the personal data intended for the assessment of the financial situation, ability to keep a commitment or credibility of a private individual; and

(9) *credit data file* means a file containing personal credit data.

Section 4 — *Application of Finnish law*

(1) This Act applies to processing of personal data where the controller is established in the territory of Finland or otherwise subject to Finnish law.

(2) This Act applies also if the controller is not established in the territory of a Member

State of the European Union, but it uses equipment located in Finland in the processing of personal data, except where the equipment is used solely for the transfer of data through the territory. In this case the controller shall designate a representative established in Finland.

## Chapter 2 — **General rules on the processing of personal data**

### Section 5 — *Duty of care*

The controller shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject's private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an Act. Anyone operating on the behalf of the controller, in the form of an independent trade or business, is subject to the same duty of care.

### Section 6 — *Defined purpose of processing*

It must be appropriate and justified to process personal data in the operations of the controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or their organisation into a personal data file. The purpose of the processing shall be defined so that those operations of the controller in which the personal data are being processed are made clear.

### Section 7 — *Exclusivity of purpose*

Personal data must not be used or otherwise processed in a manner incompatible with the purposes referred to in section 6. Later processing for purposes of historical, scientific or statistical research is not deemed incompatible with the original purposes.

### Section 8 — *General prerequisites for processing*

(1) Personal data shall be processed only if:

(1) the data subject has unambiguously consented to the same;

(2) the data subject has given an assignment for the same, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(3) processing is necessary, in an individual case, in order to protect the vital interests of the data subject;

(4) processing is based on the provisions of an Act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of an Act or an order issued on the basis of an Act;

(5) there is a relevant connection between the data subject and the operations of the controller, based on the data subject being a client or member of, or in the service of, the controller or on a comparable relationship between the two (*connection requirement*);

(6) the data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping,

(7) processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;

(8) the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the controller or a third party receiving the data; or

(9) the Data Protection Board has issued a permission for the same, as provided in section 43(1).

Personal data may be disclosed on the basis of paragraph (1)(5) only if such disclosure is a regular feature of the operations concerned and if the purpose for which the data is disclosed is not incompatible with the purposes of the processing and if it can be assumed that the data subject is aware of such disclosure.

Chapter 3 contains provisions on the processing of sensitive personal data and personal identity numbers. Chapter 4 contains provisions on the processing of personal data for special purposes.

The provisions on access to official documents apply to access to information in the personal data files of the authorities and to other disclosure of. personal data therein.

Section 9 — *Principles relating to data quality*

(1) The personal data processed must be necessary for the declared purpose of the processing (*necessity requirement*).

(2) The controller shall see to that no erroneous, incomplete or obsolete data are processed (*accuracy requirement*). This duty of the controller shall be assessed in the light of the purpose of the personal data and the effect of the processing on the protection of the privacy of the data subject.

Section 10 — *Description of file*

(1) The controller shall draw up a description of the personal data file, indicating:
   (1) the name and address of the controller and, where necessary, those of the representative of the controller;
   (2) the purpose of the processing of the personal data;
   (3) a description of the group or groups of data subjects and the data or data groups relating to them;
   (4) the regular destinations of disclosed data and whether data are transferred to countries outside the European Union or the European Economic Area; and
   (5) a description of the principles in accordance to which the data file has been secured.

(2) The controller shall keep the description of the file available to anyone. This obligation may be derogated from, if necessary for the protection of national security, defence or public order and security, for the prevention or investigation of crime, or for a supervision task relating to taxation or public finances.

Chapter 3 — **Sensitive data and personal identity number**

Section 11 — *Prohibition to process sensitive data*

The processing of sensitive data is prohibited. Personal data are deemed to be sensitive, if they relate to or are intended to relate to:
   (1) race or ethnic origin;
   (2) the social, political or religious affiliation or trade-union membership of a person;
   (3) a criminal act, punishment or other criminal sanction;
   (4) the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person;
   (5) the sexual preferences or sex life of a person; or
   (6) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.

Section 12 — *Derogations from the prohibition to process sensitive data*

(1) The prohibition in section 11 does not prevent:
   (1) processing of data where the data subject has given an express consent;
   (2) processing of data on the social, political or religious affiliation or trade-union membership of a person, where the person has himself/herself brought the data into the public domain;
   (3) processing of data necessary for the safeguarding of a vital interest of the data subject or someone else, if the data subject is incapable of giving his/her consent;
   (4) processing of data necessary for drafting or filing a lawsuit or for responding to or deciding of such a lawsuit;
   (5) processing of data where based on the provisions of an Act or necessary for compliance with an obligation to which the controller is subject directly by virtue of an Act;
   (6) processing of data for purposes of historical, scientific or statistical research;
   (7) the processing of data on religious, political or social affiliation in the operations of an association or corporation professing such affiliation, where the data relate to members of the association or corporation or to persons connected to the association or

corporation on a regular basis and in the context of the stated purposes of the association or corporation, and where the data is not disclosed to a third party without the consent of the data subject;

(8) the processing of data on trade-union membership in the operations of a trade union or a federation of trade unions, where the data relate to the members of the union or federation or to persons connected to the union or federation on a regular basis and in the context of the stated purposes of the union or federation, and where the data is not disclosed to a third party without the consent of the data subject;

(9) the processing of data on trade-union membership, where necessary for the observation of the special rights and duties of the controller in the field of labour law;

(10) a health care unit or a health care professional from processing data collected in the course of their operations and relating to the state of health, illness or handicap of the data subject or the treatment or other measures directed at the data subject, or other data which are indispensable in the treatment of the data subject;

(11) an insurer from processing data collected in the course of its insurance activity and relating to the state of health, illness or handicap of the policyholder/claimant or the treatment or other measures directed at the policyholder/claimant, or data on the criminal act, punishment or other sanction of the policyholder/claimant or the person causing the damage, where necessary for the determination of the liability of the insurer;

(12) a social welfare authority or another authority, institution or private producer of social services granting social welfare benefits from processing data collected in the course of their operations and relating to the social welfare needs of the data subject or the benefits, support or other social welfare assistance received by the person or otherwise indispensable for the welfare of the data subject; or processing of data where the Data Protection Board has issued a permission for the same, as provided in section 43(2).

(2) Sensitive data shall be erased from the data file immediately when there no longer is a reason for its processing, as provided in paragraph (1). The reason and the need for processing shall be re-evaluated at five-year intervals at the longest, unless otherwise provided in an Act or stated in a permission of the Data Protection Board referred to in paragraph (1)(13).

Section 13 — *Processing of a personal identity number*

(1) A personal identity number may be processed on the unambiguous consent of the data subject or where so provided in an Act. A personal identity number may also be processed if it is necessary to unambiguously identify the data subject:
   (1) in order to perform a task laid down in an Act;
   (2) in order to realise the rights or duties of the data subject or the controller; or
   (3) for purposes of historical, scientific or statistical research.

(2) A personal identity number may be processed in activities relating to the granting of credit and the collection of debt, in the insurance, credit, renting and lending businesses, in credit data operations, in health care, in social welfare activities or other social services and in matters relating to the civil service, employment and other service relationships and benefits relating to the same.

(3) In addition to the provisions on processing in paragraphs (1) and (2), a personal identity number may be disclosed for the purposes of updating of address information and prevention of redundant postal traffic, provided that the personal identity number is already available to the recipient.

(4) The controller shall see to that the personal identity number is not unnecessarily included in hard copies printed or drawn up from the personal data file.

## Chapter 4 — **Processing of personal data for special purposes**

Section 14 — *Research*

(1) Personal data may be processed for purposes of historical or scientific research also for a reason not referred to in section 8(1), if:
   (1) the research cannot be carried out without data identifying the person and the consent of the data subjects cannot be obtained owing to the quantity of the data, their age or

another comparable reason;

(2) the use of the personal data file is based on an appropriate research plan and a person or a group of persons responsible for the research have been designated;

(3) the personal data file is used and data are disclosed therefrom only for purposes of historical or scientific research and the procedure followed is also otherwise such that the data pertaining to a given individual are not disclosed to outsiders; and

(4) after the personal data are no longer required for the research or for the verification of the results achieved, the personal data file is destroyed or transferred into an archive, or the data in it are altered so that the data subjects can no longer be identified.

(2) The provision in paragraph (1)(3) does not apply if the procedure in that paragraph is manifestly unnecessary for the protection of the privacy of the data subjects owing to the age or quality of the data in the personal data file.

(3) The provisions in paragraph (1) apply in a supplementary manner where the processing of the personal data is based in section 8(1).

Section 15 — *Statistics*

Personal data may be processed for statistical purposes also for a reason not referred to in section 8(1), if:

(1) the statistics cannot be compiled or the underlying data requirements fulfilled without using personal data;

(2) the compilation of statistics is an activity where the controller is engaged in; and

(3) the file is used for statistical purposes only and data are not disclosed from it in a way allowing for the identification of a given individual, except where the data are disclosed for official statistics.

Section 16 — *Official plans and reports*

For purposes of official planning and reporting, an authority may collect and record personal data, also for a reason not referred to in section 8(1), into an official personal data file; in this event, the provisions in section 14 apply in so far as appropriate.

Section 17 — *Public registers*

(1) Unless prohibited by the data subject, data may be collected and recorded, also for a reason not referred to in section 8(1), into a personal data file kept for purposes of a public register, as follows: identifying data on the data subject, his/her spouse, children and parents, data on the connecting factor on the basis of which the public register has been compiled and related data, as well as the data subject's contact information.

(2) Here a public register means a publication where the data subjects are connected by a given profession or education, by the membership of a professional body or other community or by status or achievement in culture, sports, business or other civic activity, or by another comparable circumstance.

(3) For purposes of a public register referred to in paragraph (1), data that may under that paragraph be collected and recorded into such a file may be disclosed from another file, unless prohibited by the data subject.

Section 18 — *Genealogical research*

(1) Unless prohibited by the data subject, data may be collected and recorded, also for a reason not referred to in section 8(1), into a personal data file kept for the purposes of genealogical research, as follows: identifying data on the member of a family and his/her spouse, the other data required for genealogical research and the data subject's contact information.

(2) For purposes of a genealogical register referred to in paragraph (1), data that may under that paragraph be collected and recorded into such a file may be disclosed from another file, unless prohibited by the data subject.

Section 19 — *Direct marketing and other personalised mailing*

(1) Unless such processing has been prohibited by the data subject, personal data may be collected and recorded, also for a reason not referred to in section 8(1), into a personal data file kept for

the purposes of direct marketing, distance selling, other direct advertising, opinion polling and market research or for other comparable personalised mailing, if:

(1) the personal data file is used in a predetermined and short-term marketing campaign or other measure referred to in this paragraph and its contents do not compromise the protection of the privacy of the data subject; or

(2) the personal data file contains data solely on the name, title or occupation, age, sex and native language of the data subject as well as one distinguishing datum and the data subject's contact information;

(3) the file contains data pertaining to the duties or status of the data subject in business or public life, and it is used for the mailing of information relevant to the same.

(2) For a purpose referred to in paragraph (1), data referred in paragraph (1)(2) may be disclosed or used as sample criteria in a disclosure, unless the data subject has prohibited disclosure and if it is evident that the data subject is aware of such disclosure.

Section 20 — *Processing of personal credit data*

(1) A person engaged in credit data activity may record into a credit data file the name and contact information on a person, as well as data on a default in payment or performance, where:

(1) the default has been established by a judgment or judgment by default handed down by a court and no longer subject to appeal, by a measure undertaken by the enforcement authorities or by the protest of a registered bill of exchange; or the default has led to the official declaration of the insolvency of the data subject in enforcement proceedings;

(2) the default has led to the filing of a bankruptcy petition;

(3) the default has been acknowledged in writing by the data subject to the creditor; or

(4) the default relates to a hire-purchase scheme and under the Hire-Purchase Act (91/1966) entitles the seller to repossess the object, or relates to another consumer credit agreement and under the Consumer Protection Act (38/1978) entitles the creditor to terminate the agreement.

(2) The data referred to above in paragraph (1)(4) may be recorded only if there is a clause in the consumer credit agreement stating the situations in which the default in payment or performance can be recorded into the credit data file. Further prerequisites are that the creditor has at least 21 days earlier sent the debtor a written reminder which mentions the possibility of recording default data into the credit data file and that the debtor has been in default for at least 60 days from the original due date, mentioned in the reminder.

(3) In addition, data may be recorded in a credit data file on the entries contained in the debt adjustment register referred to in section 87 of the Act on the Adjustment of the Debts of a Private Individual (57/1993), on the placement of a person under guardianship and on the appointment of a trustee to administer the financial affairs of a person, and, on the request of the data subject, on the payment of the debt referred to in paragraph (1) and on a credit stoppage, where supplied by the data subject himself/herself.

(4) Personal credit data may be disclosed only to a controller engaged in credit data activity and to a person needing the data for purposes of granting credit or credit monitoring, or for another comparable purpose.

Section 21 — *Erasure of data in a credit data file*

The data referred to in section 20(1)(1)—(4) shall be erased from the credit data register as follows:

(1) the data referred to in subparagraph (1) after the lapse of four years from the establishment of the default;

(2) the data referred to in subparagraph (2) after the lapse of five years from the filing of the bankruptcy application;

(3) the data referred to in subparagraph (3) at the latest after the lapse of two years from the acknowledgement of the default; and

(4) the data referred to in subparagraph (4) at the latest after the lapse of two years from the recording of the entry on default.

Chapter 5 — **Transfer of personal data to outside the European Union**

Section 22 — *General prerequisites*

(1) Personal data may be transferred to outside the European Union or the European Economic Area only if the country in question guarantees an adequate level of data protection.

(2) The adequacy of the level of data protection shall be evaluated in the light of the nature of the data, the purpose and duration of the intended processing, the country of origin and the country of final destination, as well as the general and sectoral legal provisions, codes of conduct and security measures applied in that country.

Section 22a – *Findings of the Commission* (986/2000)

(1) Personal data may be transferred out of the territory of the member states of the European Union or out of the European Economic Area in so far as the Commission of the European Communities has found, pursuant to Articles 3 and 25(6) of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in the following, the *Data Protection Directive*), that the country in question guarantees an adequate level of data protection.

(2) Personal data shall not be transferred out of the territory of the member states of the European Union nor out of the European Economic Area in so far as the Commission has found, pursuant to Articles 3 and 25(4) of the Data Protection Directive, that the country in question does not guarantee an adequate level of data protection.

Section 23 — *Grounds for derogation*

Sections 22 and 22a do not prevent the transfer of data if: (986/2000):

(1) the data subject has unambiguously consented to the transfer;

(2) the data subject has given an assignment for the transfer, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(3) the transfer is necessary in order to make or perform an agreement between the controller and a third party and in the interest of the data subject;

(4) the transfer is necessary in order to protect the vital interests of the data subject;

(5) the transfer is necessary or called for by law for securing an important public interest or for purposes of drafting or filing a lawsuit or for responding to or deciding such a lawsuit;

(6) the transfer is made from a file, the disclosure of data from which, either generally of for special reasons, has been specifically provided in an Act; (986/2000)

(7) the controller, by means of contractual terms or otherwise, gives adequate guarantees of the protection of the privacy and the rights of individuals, and the Commission has not found, pursuant to Articles 3 and 26(3) of the Data Protection Directive, that the guarantees are inadequate; or (986/2000)

(8) the transfer is made by using standard contractual clauses as adopted by the Commission in accordance with Article 26(4) of the Data Protection Directive. (986/2000)

Chapter 6 — **The data subject's rights**

Section 24 — *Information on the processing of data*

(1) When collecting personal data, the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. This information shall be provided at the time of collection and recording of the data or, if the data are obtained from elsewhere than the data subject and intended for disclosure, at the latest at the time of first disclosure of the data.

(2) The duty of providing information, referred to above in paragraph (1), may be derogated from:
   (1) if the data subject already has the relevant information;
   (2) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or
   (3) where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data.

Section 25 — *Information on the processing of data in certain situations*

(1) A controller shall provide the data subject with the data contained in the credit data file and pertaining to the data subject, as well as with the information on the controller and the processing referred to in section 24, at the time when the first entry on the data subject under section 20 has been recorded into the file.
(2) Anyone who has obtained personal credit data on the data subject for the purpose of making a decision pertaining to the data subject shall notify the data subject of the use of the credit data in the decision-making, of the file from which the data have been obtained, of the time when the data have been obtained, if the rejection of credit or another decision negative from the point of view of the data subject is based on the credit data.
(3) Where the name and contact information of an individual have been obtained from a personal data file for the purposes of direct marketing, distance selling or other direct advertising, or of market research or an opinion poll, or for a comparable addressed delivery, the file used, the controller and the address of the controller shall be mentioned. A teleseller shall give the same information upon request.

Section 26 — *Right of access*

(1) Regardless of secrecy provisions, everyone shall have the right of access, after having supplied sufficient search criteria, to the data on him/her in a personal data file, or to a notice that the file contains no such data. The controller shall at the same time provide the data subject with information of the regular sources of data in the file, on the uses for the data in the file and the regular destinations of disclosed data. Where an automated decision referred to in section 31 is involved, the data subject shall also have the right of access to information on the operating principles of the pertinent automatic processing of data.
(2) A controller engaged in credit data activity shall upon the request of the data subject provide information on the recipients and destinations of personal credit data on the data subject disclosed during the preceding six months, as well as the sources of the data on the data subject.
(3) The controller may charge for the provision of access to the data only if less than one year has passed since the previous instance of providing the data subject with access to data in the file. The charge shall be reasonable and it shall not exceed the immediate costs of providing access to the data.

Section 27 — *Restrictions on the right of access*

(1) There is no right of access, as referred to in section 26 above:
   (1) if providing access to the data could compromise national security, defence or public order or security, or hinder the prevention or investigation of crime;
   (2) if providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else;
   (3) if the data in the file are used solely for historical or scientific research or statistical purposes; or
   (4) if the personal data in the file are used in the carrying out of monitoring or inspection functions and not providing access to the information is indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union.

(2) If only a part of the data on a data subject is such that it falls within the restriction on the right of access provided in paragraph (1), the data subject shall have the right of access to the remainder of the data.

Section 28 — *Realisation of the right of access*

(1) Anyone who wishes to have access to the data on himself/herself, as referred to in section 26, shall make a request to this effect to the controller by a personally signed or otherwise comparably verified document or by appearing personally in the premises of the controller.

(2) The controller shall without undue delay reserve the data subject an opportunity to inspect the data referred to in section 26 or, upon request, provide a hard copy of the data. The data shall be given in an intelligible form. If the controller refuses to provide access to the data, a written certificate to this effect shall be issued. The certificate shall also mention the reasons for the refusal. A failure by the controller to give a written response to the data subject within three months of the request is deemed equivalent to a refusal to provide access to the data. In this event, the data subject may bring the matter to the attention of the Data Protection Ombudsman.

(3) Anyone who wishes to have access to the data on himself/herself in the files of the health care authorities and institutions, physicians and dentists or other health care professionals and relating to their state of health or illness, shall make a request to this effect to a physician or another health care professional, who shall then see to the obtainment of the data with the consent of the data subject and provide him/her with access to the entries in the file.. The provisions in paragraph (2) apply to the procedure in the realisation and refusal of the right of access.

Section 29 — *Rectification*

(1) The controller shall, on its own initiative or at the request of the data subject, without undue delay rectify, erase or supplement personal data contained in its personal data file and erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing. The controller shall also prevent the dissemination of such data, if this could compromise the protection of the privacy of the data subject or his/her rights.

(2) If the controller refuses the request of a data subject of the rectification of an error, a written certificate to this effect shall be issued.The certificate shall also mention the reasons for the refusal. In this event, the data subject may bring the matter to the attention of the Data Protection Ombudsman.

(3) The controller shall notify the rectification to the recipients to whom the data have been disclosed and to the source of the erroneous personal data. However, there is no duty of notification if this is impossible or unreasonably difficult.

Section 30 — *Right to prohibit processing*

A data subject has the right to prohibit the controller to process personal data for purposes of direct advertising, distance selling, other direct marketing, market research, opinion polls, public registers or genealogical research.

Section 31 — *Automated decisions*

The making of a decision on the basis of certain characteristics of a data subject, where involving solely automatised data processing and having legal consequences to the data subject or otherwise significantly affecting him/her, is permitted only if

(1) so provided in an Act; or

(2) the decision is made in connection with the making or performance of an agreement, provided that the protection of the rights of the data subject is guaranteed or that the decision fulfils the request of the data subject on the making or performance of the agreement.

## Chapter 7 — **Data security and storage of personal data**

### Section 32 — *Data security*

(1) The controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. The techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures.

(2) Anyone who as an independent trader or business operates on the behalf of the controller shall, before starting the processing of data, provide the controller with appropriate commitments and other adequate guarantees of the security of the data as provided in paragraph (1).

### Section 33 — *Secrecy obligation*

Anyone who has gained knowledge of the characteristics, personal circumstances or economic situation of another person while carrying out measures relating to data processing shall not disclose the data to a third person against the provisions of this Act.

### Section 34 — *Destruction of a personal data file*

If a personal data file is no longer necessary for the operations of the controller, it shall be destroyed, unless specific provisions have been issued by an Act or by lower-level regulation on the continued storage of the data contained therein or the file is transferred to be archived in accordance with section 35.

### Section 35 — *Transfer of personal data to be archived*

(1) Separate provisions apply to the use and protection of personal data files which have been transferred to the possession of the archive authorities, as well as to the disclosure of data from such files. However, when disclosing personal data from a private file, the archive authority shall take into account the provisions in this Act on the processing and disclosure of personal data, unless this, in view of the age or nature of the data recorded in the file, is manifestly unnecessary for the protection of the privacy of the data subjects.

(2) A personal data file which is significant for purposes of scientific research or otherwise may be transferred for archiving to an institution of higher education or to a research institute or authority operating on a statutory basis, where the National Archives have granted a permission for such archiving. The National Archives may grant corporations, foundations and institutions a permission to archive personal data files compiled in their own activities and fulfilling the requirements above. In the permission the National Archives shall lay down rules for the protection of the files and for the monitoring of the use of the personal data.

(3) Before granting a permission referred to in paragraph (2). the National Archives shall reserve the Data Protection Ombudsman an opportunity to issue an opinion on the matter.

## Chapter 8 — **Notification to the Data Protection Ombudsman**

### Section 36 — *Duty of notification*

(1) The controller shall notify the Data Protection Ombudsman of automated data processing by sending a description of the file to that authority.

(2) In addition, the controller shall notify the Data Protection Ombudsman of:

(1) the transfer of personal data to outside the European Union or the European Economic Area, if the data are transferred on the grounds provided in section 22 or 23(6) or (7) and there is no statutory provision on the same; or

(2) the launching of an automated decision-making system referred to in section 31.

(3) Anyone who is engaged in credit data activity or carrying out debt collection or market or opinion research as a business, or operating in recruitment, personnel assessment or computing on the behalf of another, and who uses or processes files or personal data in this activity, shall

notify the same to the Data Protection Ombudsman.

(4) The duty of notification referred to above in paragraph (1) does not apply, if the processing of personal data is based on section 8(1)(1)—(3), on section 8(1)(4) if so provided by law, on a client or service relationship or membership referred to in section 8(1)(5), on section 8(1)(6) or (9), on section 12(1)—(4), on section 12(5) if so provided by law, on section 12(7)—(10), (12) or (13), or on sections 13—18 or 20. The duty of notification may also be derogated from as provided by Decree, if it is evident that the processing of personal data does not compromise the protection of the privacy of the data subject, or his/her rights or freedoms.

Section 37 — *Notification*

(1) The notification referred to above in section 36(2)(1) shall indicate the information contained in the description of the file and also the types of data being transferred and how the transfer is carried out.

(2) The notification referred to above in section 36(2)(2) shall indicate the information contained in the description of the file and also the logical construction of the system.

(3) The notification referred to above in section 36(3) shall indicate the name, field of business, domicile and address of the trader or business, the personal data files used in the activity and the type of data contained therein, the disclosure of data from the file, the duration of storage of recorded data, the technical measures for securing the data and the measures for monitoring the use of the personal data files.

(4) The notification shall be made well in advance of the collection or recording of the data to be recorded into the file or of the carrying out of another measure giving rise to the duty of notification; in any event, it shall at the latest be made 30 days before the same.

## Chapter 9 — **Direction and supervision of the processing of personal data**

Section 38 — *Data protection authorities*

(1) The Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing in order to achieve the objectives of this Act, as well as makes decisions, as provided in this Act.

(2) The Data Protection Board deals with questions of principle relating to the processing of personal data, where these are significant to the application of this Act, as well as makes decisions in matters of data protection, as provided in this Act.

(3) The data protection authorities may use the powers provided in this chapter even if the processing of personal data is according to section 4 not subject to the provisions of this Act. The data protection authorities co-operate with the data protection authorities in other Member States of the European Union, providing executive assistance, where necessary.

Section 39 — *Data protection authorities' right of access and inspection*

(1) Regardless of confidentiality provisions, the Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. The Data Protection Board has the same right in matters which it is dealing with.

(2) The Data Protection Ombudsman has the right to inspect personal data files and to assign experts to carry out the inspection. For purposes of the inspection, the Data Protection Ombudsman and an expert have the right to enter the premises of the controller and a person operating on the behalf of the controller, where personal data are processed or personal data files are kept in such premises, and to access the information and equipment required for carrying out the inspection. In premises covered by the provisions on the sanctity of the home, an inspection may be carried out only if in the matter at hand there is a specific reason to believe that the provisions on the processing of personal data have been violated or are going to be violated. The inspection shall be carried out so that it does not cause undue inconvenience or cost to the controller.

(3) As regards processing referred to in section 2(5) above, the Data Protection Ombudsman supervises compliance with the obligation to protect the data, provided in section 32. For this purpose, the Data Protection Ombudsman has the right of access to the necessary information on the protection of the data.

Section 40 — *Measures of the Data Protection Ombudsman*

(1) The Data Protection Ombudsman shall promote good processing practice and issue directions and guidelines so as to achieve a situation where unlawful conduct is not continued or repeated. Where necessary, the Data Protection Ombudsman shall refer the matter to be dealt with by the Data Protection Board, or report it for prosecution.

(2) The Data Protection Ombudsman shall decide matters brought to his/her attention by data subjects on the basis of sections 28 and 29. The Ombudsman may order a controller to realise the right of access of the data subject or to rectify an error.

(3) The Data Protection Ombudsman may issue more detailed guidelines on how personal data is to be secured against unlawful processing.

Section 41 — *Hearing the Data Protection Ombudsman*

(1) The authority concerned shall reserve the Data Protection Ombudsman an opportunity to be heard in connection with the drafting of legislative or administrative reforms relating to the protection of personal rights or freedoms in the processing of personal data.

(2) Before bringing charges for conduct contrary to this Act, the public prosecutor shall hear the Data Protection Ombudsman. When hearing a case of this sort, the court shall reserve the Data Protection Ombudsman an opportunity to be heard.

Section 42 — *Sectoral codes of conduct*

Controllers or their representatives may draft sectoral codes of conduct for the application of this Act and the promotion of good processing practice, and send these to the Data Protection Ombudsman. The Data Protection Ombudsman may check if the code of conduct is in conformity with this Act and the other provisions relating to the processing of personal data.

Section 43 — *Power of the Data Protection Board to grant permissions*

(1) The Data Protection Board may grant a permission for the processing of personal data, as referred to in section 8(1)(9), if the processing is necessary, otherwise than in an individual case, in order to protect the vital interests of the data subject, or in order to use the public authority of the controller or a third person to whom the data is to be disclosed. The permission may be granted also in order to realise a legitimate interest of the controller or the recipient of the data, provided that such processing does not compromise the protection of the privacy of the individual or his/her rights.

(2) The Data Protection Board may grant a permission for the processing of sensitive data, as referred to in section 12(13), for a reason pertaining to an important public interest.

(3) The permission may be granted for a fixed period or for the time being; it shall contain the rules necessary for the protection of the privacy of the data subject. These rules may be amended or supplemented at the request of the Data Protection Ombudsman or the data subject, if this is necessary owing to a change in circumstances.

Section 44 — *Orders of the Data Protection Board*

At the request of the Data Protection Ombudsman, the Data Protection Board may:

(1) prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act;

(2) in matters other than those referred to in section 40(2), compel the person concerned to remedy an instance of unlawful conduct or neglect;

(3) order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme; and

(4) revoke a permission referred to in section 43, where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it.

Section 45 — *Appeal*

(1) The decisions of the Data Protection Ombudsman, referred to in section 40(2), and the Data Protection Board, referred to in sections 43 and 44, are subject to appeal in accordance with the provisions of the Administrative Judicial Procedure Act (586/1996). The Data Protection Ombudsman may appeal against the decision of the Data Protection Board, referred to in section 43.

(2) It may be ordered in a decision of the Data Protection Board that it is to be complied with regardless of appeal, unless otherwise ordered by the appellate authority.

Section 46 — *Threat of a fine*

The Data Protection Ombudsman may impose a threat of a fine, in accordance with the Act on Threats of a Fine (1113/1990), in order to reinforce the duty to provide access to data, as referred to in section 39(1) and 39(3), and a decision made on the basis of section 40(2); the Data Protection Board may do likewise in relation to the duty to provide access to data, as referred to in section 39(1), and a decision made on the basis section 44.

Chapter 10 — **Miscellaneous provisions**

Section 47 — *Liability in damages*

(1) The controller is liable to compensate for the economic and other loss suffered by the data subject or another person because of processing of personal data in violation of the provisions of this Act.

(2) Otherwise the provisions in chapter 2, sections 2 and 3, chapter 3, sections 4 and 6 and chapters 4, 6 and 7 of the Damages Act (412/1974) apply to the liability in damages.

Section 48 — *Penal provisions*

(1) The penalty for a personal data offence is provided in chapter 38, section 9 of the Penal Code (39/1889) and for breaking into a personal data file in chapter 38, section 8 of the Penal Code. The penalty for a violation of the secrecy obligation referred to in section 33 is provided in chapter 38, section 1 or 2 of the Penal Code, unless the act is punishable under chapter 40, section 5 of the Penal Code or a more severe penalty is provided in another Act.

(2) A person who intentionally or grossly negligently and contrary to the provisions in this Act:

(1) fails to comply with the provisions on the definition of the purpose of the processing of the personal data, the drawing up of the description of the file, the information on data processing, the rectification of the file, the right of the data subject to prohibit the processing of data or the notification of the Data Protection Ombudsman;

(2) provides false or misleading data to a data protection authority in a matter concerning a personal data file;

(3) breaks the rules or regulations on the protection and destruction of personal data files; or

(4) breaks a final order issued by the Data Protection Board on the basis of section 43(3),

thus compromising the protection of the privacy of the data subject or his/her rights, shall be sentenced for a *personal data violation* to a fine, provided that a more severe penalty is not provided in another Act.

Section 49 — *Further provisions*

Further provisions on the enforcement of this act are issued by Decree.

Chapter 11 — **Entry into force and transitional provisions**

Section 50 — *Entry into force*

(1) This Act enters into force on 1 June 1999.

(2) This Act repeals the Personal Data File Act (471/1987), as later amended. However, the

provisions of the repealed Act on mass deliveries and sensitive samples continue to apply, in so far as referred to in other legislation, until 24 October 2001.

(3) Measures necessary for the implementation of this Act may be undertaken before its entry into force.

Section 51 — *Transitional provisions*

(1) Processing of personal data commenced before the entry into force of this Act shall be modified so as to comply with the provisions of this Act at the latest on 24 October 2001.

(2) A reference elsewhere in law to the repealed Personal Data File Act or its provisions shall be deemed to be a reference to this Act or its corresponding provisions.