

## 523/1999

Done at Helsinki on 22 April 1999

### The Personal Data Act

In accordance with a decision of Parliament:

#### Chapter 1

##### General provisions

###### 1 §

###### Purpose of the Act

The purpose of this law is to implement the fundamental rights protecting privacy and other privacy in the processing of personal data and to promote the development and observance of good data processing practices.

#### Section 2

##### Scope of application

In the processing of personal data, the provisions of this Act shall be complied with, unless otherwise provided in other laws.

This law applies to the automatic processing of personal data. Also, other personal data processing is governed by this law when personal data are or are intended to constitute a personal register or part thereof.

This law does not apply to the processing of personal data by a natural person solely for personal or similar normal private purposes.

This law does not apply to personal registers which contain only material published in the media as such.

Articles 1-4 and 32, Section 39, subsection 3., 40 Section 1 and 3 mom., Section 42, Section 44 Section 2, 45-47 shall apply *mutatis mutandis* to the processing of personal data for editorial purposes and for the purposes of artistic or literary expression Section 48, subsection 2. And 50 and 51 Section, subject to Section 17.

#### Section 3

##### Definitions

For the purposes of this Act:

- (1) *personal data* of any nature or of his characteristics or living conditions which may be identified by him or his family or with his or her family living in the same household;
- 2) *processing of personal data concerning* the collection, deposit, organization, use, transfer, disclosure, preservation, modification, merger, protection, deletion, destruction and other personal data of personal data;
- 3) personal data contained in the personal *register for the* purposes of their *personal* use for the purposes of their personal data, which is processed partly or wholly by automatic data processing or which is organized as an index, list or other comparable means,

- 4) the *controller* of one or more persons, entities, institutions or foundations for the use of which a register of persons is established and which has the right to order the use of a personal register or to which the register is regulated by law;
- 5) the *registered* person concerned by the personal data;
- 6) any *third* person, entity, institution or foundation other than a registrar, registrar, personal data handler or personal data relating to the last two;
- 7) *with the agreement* of any kind of voluntary, individualized and conscious expression of will by which the registrar accepts the processing of his or her personal data;
- 8) The *personal credit information*, personal data are intended for use in the assessment of the private natural person's economic status, repayment capacity or the reliability of the commitments; mixed
- 9) a *credit* register with a register of personal *credit data* .

#### **Section 4**

##### **Application of Finnish law**

This law applies to the processing of personal data in which the registrar has its registered office in Finland or otherwise within Finnish jurisdiction.

This law also applies where the controller does not have an establishment in the territory of the Member States of the European Union, but the controller uses personal data for processing in Finland for purposes other than data transfer through that territory. The registrar must then designate a representative in Finland.

## **Chapter 2**

### **General principles for the processing of personal data**

#### **Section 5**

##### **Duty of care**

The controller should treat legitimate personal data, observe diligence and good computing, and otherwise act in such a way that the privacy of the data subject's privacy and other fundamental rights protecting privacy can not be restricted without the statutory provision. The same obligation is that of an independent business or operator acting on behalf of a controller.

#### **Section 6**

##### **Design of personal data processing**

The processing of personal data must be reasonably justified for the operations of the controller. The purposes for which personal data are processed and where personal data are regularly acquired and to which they are ordinarily disclosed must be defined before the personal data is collected or constituted as a personal register. The purpose of processing personal data should be defined in such a way as to indicate the types of personal data that are processed by the data controller.

#### **Section 7**

##### **purpose limitation**

Personal data may only be used or otherwise processed in a manner that is not incompatible with the purposes of the processing referred to in section 6. Later processing of personal data for historical, scientific or statistical purposes is not considered incompatible with the purpose of the original processing.

#### **Section 8**

##### **General conditions for handling**

Personal data may only be processed:

- 1) with the explicit consent of the data subject;
- 2) a registered assignment or enforcement of an agreement in which the data subject is a party, or the execution of pre-contractual measures at the request of the data subject;
- (3) where processing in an individual case is necessary to protect the data subject's vital interest;
- 4) if the processing is regulated by law or if the processing is due to the controller or the obligation or obligation prescribed by law or under the law;
- 5) if the data subject has a proper connection with the controller ( *connection requirement* ) because of the customer, service, membership or other comparable relationship ;
- 6) if the question is about the customers or employees of a group or other economic association and that information is processed within that consortium;
- 7) where processing is necessary for the payment service, data processing or other comparable tasks performed by the controller;
- 8) where the question is about publicly available information describing the status, tasks and management of the person in the public sector or the business, and this information is processed to safeguard the controller's or third party rights and interests; or
- 9) if the Data Protection Board has handled the authorization referred to in section 43, subsection 1.

The disclosure of personal data may only be effected pursuant to subsection 1 (5) if the disclosure of personal data is a normal part of the exercise of the activity concerned, provided that the purpose for which the information is disclosed is not incompatible with the purpose of processing the personal data and that the data subject may be expected to know that such disclosure.

The treatment of sensitive personal data and personal identification number is provided in Chapter 3. The processing of personal data for specific purposes is governed by Chapter 4.

The right to obtain information and other personal data from the Authority's personal register is governed by the publicity of public authorities.

## **Section 9**

### **Principles of data quality**

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

The registrar must ensure that no inaccurate, obsolete or outdated personal data is processed (due *diligence* ). When assessing the obligation of a controller, account must be taken of the purpose of processing personal data and the importance of processing for the protection of registered privacy.

## **Section 10**

### **Privacy**

The registrar must draw up a Register Statement from the Register of Persons, which shows:

- 1) the name and contact details of the controller and, where applicable, his representative;
- 2) the purpose of processing personal data;
- 3) a description of the registered group or groups and the related data or data groups;

(4) what information is regularly transmitted and whether information is transmitted outside the European Union or the European Economic Area; mixed

5) a description of the principles of the protection of the registry.

The Registry must keep the Privacy Policy available to everyone. This obligation may be waived if it is necessary for State security, defense or public order and security, for the purpose of preventing or detecting crimes, or for fiscal or fiscal control purposes.

### **Chapter 3**

#### **Sensitive information and personal identity number**

##### **Section 11**

##### **Prohibition of sensitive data processing**

Processing of sensitive personal data is prohibited. Sensitive information is considered to be personal data that describes or is intended to describe:

- 1) race or ethnic origin;
- 2) a person's social, political or religious belief or belonging to a trade union;
- 3) criminal offense, punishment or other criminal offense;
- 4) the health, illness or disability of a person, or the treatment measures or similar actions directed against him;
- 5) the sexual orientation or behavior of a person; or
- 6) the need for social welfare of the person or the social welfare services he / she receives, support measures and other social welfare benefits.

##### **Section 12**

##### **Exceptions to the Prohibition of Sensitive Data Processing**

Article 11 does not preclude:

- 1) the processing of data to which the data subject has given his / her express consent;
- 2) the processing of information about a person's social, political or religious belief or belonging to a trade union, which the public has publicly disclosed;
- (3) the processing of data necessary to protect the vital interests of the data subject or of another person if the data subject is prevented from consent;
- (4) the processing of information necessary for the purpose of drawing up, presenting, defending or resolving legal proceedings;
- 5) the processing of data provided for in the law or directly attributable to the controller of the statutory duty;
- 6) processing of data for historical or scientific research or for statistical purposes;
- 7) the processing of information on religious, political or social beliefs in the activities of associations representing such beliefs and other entities where the information relates to members of these associations or organizations or to persons who have regular contacts with them for the purposes of associations and entities and the disclosure of information to third parties without the consent of the data subject ;
- 8) the processing of information on the membership of a trade union in the activities of trade unions and their associations if the information relates to members of such organizations or to persons who have regular

associations with organizations for purposes of organization and no information is disclosed to third parties without the consent of the data subject;

9) the processing of information on the membership of a trade union which is necessary for the observance of the special rights and obligations of the controller in the field of labor law;

10) a health care unit or a healthcare professional dealing with the information received in this activity about the health status, illness or disability of the data subject or the treatment measures assigned to him or other information necessary for the care of the data subject;

11) Information on the health, illness or disability of the insured and the claimant of the claimant, as well as information on the criminal act, punishment or other penalty of the insured person, the claimant or the perpetrator of the claim that is indispensable for determining the liability of the insured;

12) a social welfare authority or other social security service provider, an institution or a private social service provider to process information received by a public authority, institution or service provider in the course of his or her activities concerning the need for social welfare of registered or social welfare services, support measures or other social welfare benefits granted to him or other information necessary for the maintenance of the data ; or

13) the processing of data to which the Data Protection Board has issued the authorization referred to in section 43, subsection 2. Or.

Sensitive information shall be deleted from the register immediately after processing is not provided for in subsection 1. The basis and the need for processing shall be evaluated at least every five years, subject to the law or the authorization given by the Data Protection Board referred to in subsection 1, point 13.

### **Section 13 Handling the ID**

A personal identification number may be processed by the data subject explicitly with the consent of the data subject, or if the processing is regulated by law. In addition, a personal identification number may be processed if it is important to uniquely identify the data subject:

- 1) to perform a task prescribed by law;
- 2) the rights and obligations of a registered or registrar; or
- 3) for historical or scientific research or for statistical purposes.

The identity number can be processed in lending or debt collection, insurance, credit institution, leasing and lending, credit information, health care, social welfare and other social security matters or matters relating to employment, employment and other services and related interests.

In addition to what is covered by the processing of the personal identity code in subsections 1 and 2, the personal identification number may be provided for updating the address information or for multiple processing for avoiding multiple mail when the personal identity number is already available to the transferee.

The registrar shall ensure that the personal identity number is not unnecessarily labeled on documents produced or made out of the personal file.

## **Chapter 4 Handling personal data for specific purposes**

### **Section 14 Research**

For the purposes of historical or scientific research, personal data may be processed for reasons other than those provided for in section 8, subsection 1 if:

- 1) the investigation can not be carried out without the person's identification data and if the consent of the data subjects is not possible due to the large number of data, the age of data or any other reason;
- 2) the use of the personal register is based on an appropriate research plan and the research is conducted by a responsible leader or a corresponding group;
- 3) personal data are used and personal data are disclosed only for historical or scientific research and otherwise are operated so that information about a particular person is not disclosed to third parties; mixed
- 4) the personal register is destroyed or transferred to be archived or the data is changed to such a form that the subject matter of the information can not be identified when personal data are no longer necessary for the purpose of the investigation or to ensure the correctness of its results.

Paragraph 1 (3) shall not apply if the procedure referred to in the personal data in the register of persons is the age and quality of the data, which is obviously unnecessary for the privacy of the data subjects.

The provisions of subsection 1. Applicable in the case of personal data processing based on Section 8 subsection 1. Applicable in subsection 1.

#### **Section 15** **Statistics**

For statistical purposes, personal data may be processed for reasons other than those provided for in section 8, subsection 1 if:

- 1) the statistics can not be produced or the information required to carry it out without the processing of personal data;
- 2) the production of statistics is a matter for the controller; mixed
- 3) the statistical register is used for statistical purposes only and is not disclosed in such a way that a person is identifiable, unless the information is disclosed for public purposes.

#### **Section 16** **Authorities planning and clarifying tasks**

For the purposes of planning and clarification, the authority may collect and deposit personal data in the register of persons of the authority, in accordance with the provisions of Section 8 subsection 1. Section 14, *mutatis mutandis*.

#### **Section 17** **personal register**

For the purposes of the personal data contained in the register of persons, the data contained in the personal register may be collected and stored for registration and the identification data necessary for the purpose of the register, the registered data integrator and the related information, as well as the contact details of the registered and his / her spouse, The registrar has not forbidden the collection and deposit of information about himself.

A personal matrix refers to a publication in which a signatory is a particular profession or education, membership of a work or other community, or a position or achievement in culture, sport, business or other social life, or any other comparable element.

For the register of persons referred to in subsection 1 above, it is possible for the person register to disclose the information that the registrar has right to collect and deposit in such register under subsection 1 unless the data

subject has denied disclosure.

## **Section 18**

### **genealogy**

For the purposes of the statutes provided for in Article 8, subsection 1 of the Family Act, a person who is a person in the family and his / her spouse may collect and store the identification data necessary for the purpose of the register, as well as other personal data necessary for the purposes of the genealogical investigation, as well as contact details for contact, unless the data subject has denied deposit.

For the genealogy register referred to in subsection 1 above, it is possible for the person register to disclose the information that the registrar has right to collect and deposit in such register under paragraph 1 unless the data subject has denied disclosure.

## **Section 19**

### **Direct marketing and other addressable shipments**

In the personal register used for direct advertising, distance selling or other direct mail marketing, opinion or market research or other comparable addressable broadcasts, collecting and storing personal data other than those provided for in section 8, subsection 1, unless the data subject has prohibited such collection and filing of personal data,

- 1) the personal register is used for a previously identified and long-term marketing activity or any other activity referred to in this subsection and, because of its data content, does not compromise the privacy of the data subject;
- 2) the personal register contains information only on the registered name, value or profession, age, gender and mother tongue, one identifier to be associated with him and contacts for contact; or
- 3) the personal register contains information concerning the registered office and position in the business or public office and is used to send information related to his or her work.

For the purpose referred to in subsection 1 above, the personal data may be disclosed or disclosed in the transfer as the basis for the use of the information referred to in subsection 1 (2) unless the data subject has denied the disclosure of information and it is evident that the data is disclosed.

## **Section 20**

### **Handling of personal credit information**

In addition to the person's name and contact details, the credit information practitioner may store in the credit information register information about such payment or performance failure:

- 1) found by a final judgment, by a unilateral judgment, by the delivery of the enforcement authority or by the protest of a bribe approved by the registrar, or by which a registered party has been found to be unauthorized in the enforcement procedure;
- 2) which has resulted in filing for bankruptcy;
- 3) whose registered status has been acknowledged by the registered letter to the creditor; or
- 4) the seller has a right to repurchase the object or creditor under the Consumer Protection Act (38/1978) according to the Law on Charges for Sale (91/1966), the right to terminate another consumer credit agreement.

The information referred to in subsection 1 (4) may only be deposited if the consumer credit agreement indicates the circumstances in which the failure to pay or performance may be registered in the credit index. In addition, the creditor has to send the debtor at least 21 days prior to the registration of the information a written payment

notice that reminded of the possibility of registering the payment default to the credit index and that the payment has been delayed more than 60 days from the original due date mentioned in the payment request.

In addition, the credit information register may also deposit the information on the information contained in the debt settlement register referred to in section 87 of the Act on the Debt Settlement of a Private Individual (57/1993) and the declaration of a person for the purpose of patronizing or naming a person for the purpose of his financial affairs and at the request of a data subject, .

Personal credit information may only be disclosed to a data controller engaged in credit information and to those in need of information on the granting of credit or credit control or for any other comparable purpose.

## **Section 21**

### **Deletion of data from a credit index**

Information in accordance with Section 20 subsection 1. 1-4 is deleted from the credit information register as follows:

1. the information in paragraph 1 four years after the payment default has been established in accordance with paragraph 1;
- 2) the details of paragraph 2 five years after filing for bankruptcy;
3. the details of paragraph 3 no later than two years after the recognition of the default; mixed
- (4) Section 4 information no later than two years after the registration of the default.

## **Chapter 5**

### **Transfers of personal data outside the European Union**

#### **Section 22**

##### **General conditions**

Personal data may only be transferred to the territory of the Member States of the European Union or to the European Economic Area if the country concerned provides sufficient data protection.

The adequacy of the level of data protection shall be assessed taking into account the nature of the data, the purpose and duration of the intended processing, the country of origin and final destination, the general and sectoral legal rules in force in the country concerned, the code of conduct and the security measures to be followed.

#### **Section 23**

##### **Exception Basics**

Where the conditions laid down in section 22 are not met, however, personal data may be transferred if:

- 1) the data subject has given his or her unambiguous consent to the transfer;
- 2) the transfer is necessary for the purpose of signing the contract or for the execution of the agreement between the data subject and the controller or for the implementation of the pre-contractual measures at the request of the data subject;
- (3) the transfer is necessary to conclude or implement an agreement in the registered interest between the controller and the other party;
- (4) a transfer is necessary to protect the data subject's vital interest;
- (5) a transfer is necessary or required by law to safeguard an important public interest or to establish, present, defend or resolve a legal claim;



(6) the transfer is made from a register for which general or specific access to information is expressly provided;  
or

7) the controller entrusts with contractual clauses or otherwise adequate safeguards to protect the privacy and rights of individuals.

## **Chapter 6**

### **Registered Rights**

#### **Section 24**

##### **Information on the processing of data**

When collecting personal data, the controller shall ensure that the data subject can obtain information from the controller and, where appropriate, his / her representative, the purpose of the processing of personal data, and on which information is regularly disclosed, as well as the information necessary to exercise the rights of the data subject in the processing of the personal data concerned. Information shall be provided when collecting and depositing personal data, or where the information is obtained elsewhere than the data subject and the information is to be disclosed no later than when the information is first disclosed.

The information obligation provided for in subsection 1. Can be deviated from:

1) if the data subject has already received this information;

(2) if it is necessary for State security, defense or public order and security, to prevent or detect crimes or to exercise fiscal control or fiscal control; or

(3) collecting information from a non-registered user if it is impossible or unreasonable to provide the data to the data subject, or to cause harm or harm to the data subject or to the purpose of processing, or to use the data to be deposited for decision-making on registration or when data collection, deposit or disclosure is expressly provided.

#### **Section 25**

##### **Information on processing of data in certain cases**

The registrar shall notify the registered registrations in the Registered Credit Register and the data controller and data processing referred to in section 24 when the first entry in the register pursuant to Section 20 of the Register has been entered in the Credit Register.

A person who has obtained registered personal credit data for use as a registrant for registration shall notify the data subject of the use of personal credit data in decision making and where the credit information originates and when they are acquired if the denial of credit or any other negative decision is due to the personal credit information obtained.

In direct mail, distance selling and other direct marketing, as well as market research and polling polls and other comparable mailing submissions for which the person's name and contact information has been obtained from the personal register, the person's personal register, the controller and his contact details. In the telephone sales, the corresponding information must be provided on request.

#### **Section 26**

##### **The right of inspection**

Everyone, without prejudice to confidentiality rules, has the right to know the information necessary to find the information, after having been informed of the information that he or she has stored in the personal register or of the data in the register. At the same time, the controller shall inform the registered data of the regular sources of information of the registry and of the data used in the register and of the regular disclosure. In the case of an automated decision within the meaning of Section 31, the data subject has the right to be informed also of the principles of automatic processing of data.

At the request of a data subject, the credit rating data controller shall provide information on who or where personal data relating to him have been disclosed during the last six months and from whom or from whom the data relating to the data originated.

The controller may only recover the information if it has been less than one year since the last person concerned had checked the data in the register. The remuneration to be recovered shall be reasonable and shall not exceed the direct costs of providing the information.

#### **Section 27**

##### **Restrictions on the right of access**

The right of inspection referred to in section 26 shall not apply if:

(1) disclosure could damage public security, defense or public order and security or hinder the prevention or detection of criminal offenses;

(2) the disclosure of information could cause a serious risk to the health or care of the data subject or to any other rights;

3) personal data contained in the register is used solely for historical or scientific research or for statistical purposes; or

4) personal data contained in the register are used for control and inspection tasks and failure to provide information is necessary to safeguard the Finnish or European Union's important economic or financial interests.

If only a part of the registered data is such that they are excluded from the scope of subsection 1, the data subject has the right to know other information that he has deposited.

#### **Section 28**

##### **Implementation of the right of inspection**

Anyone wishing to inspect the information about themselves as referred to in section 26 must submit a request for this to the controller in a personally signed or equivalent document or in person at the Registry.

Without undue delay, the data controller shall reserve the opportunity to the data subject to access the information referred to in section 26 or, if requested, in writing. The information must be given in an understandable form. If the controller refuses to provide information, he / she must provide a written certificate. The certificate shall also state the reasons why the right of inspection has been refused. As a justification for refusal of access, it is considered that the controller has not given a written reply to the data subject within three months of the request. The Registrar may refer the matter to the Data Protection Supervisor.

A person who wishes to know what information about him has been deposited in a register containing personal data relating to health, medical or dental health, medical or dental practitioners or other healthcare professionals in a healthcare authority or institution, must apply to the physician or other healthcare professional responsible for obtaining the information With consent and give this information to the entries in the register. The procedure for enforcing or refusing the right of inspection is governed by the provisions of subsection 2.

#### **Section 29**

##### **Correcting information**

Without undue delay, the registrar shall, on his own initiative or at the request of the data subject, rectify, delete or supplement the incorrect, unnecessary, incomplete or obsolete personal data contained in the register for the purpose of processing. The registrar must also prevent the spread of such information if the information may endanger the privacy of the data subject or his rights.

Unless the registrar accepts the data subject's claim for correction of the information, he / she must issue a written certificate. The certificate shall also state the reasons why the claim has not been accepted. The Registrar may refer the matter to the Data Protection Supervisor.

The controller shall inform the data subject to whom the data controller has surrendered or where the data controller has received incorrect personal data. However, there is no obligation to notify if reporting is impossible or requires unreasonable trouble.

### **Section 30** **Right of Refusal**

The registrar has the right to deny the controller the processing of information about himself about direct mail, distance sales and other direct marketing as well as marketplace opinion polls, as well as personal identity and genealogy research.

### **Section 31** **Automated decision**

The adoption of a decision to evaluate certain characteristics of a registered data, which takes place only on the basis of automated data processing and which results in legal effects of the registration or which otherwise has a significant effect on him, shall be permitted only if:

- 1) it is provided by law; or
- (2) a decision is taken in the course of the conclusion or implementation of the contract provided that the protection of the rights of the data subject is ensured or that the decision satisfies the request for the conclusion or enforcement of a registered contract.

## **Chapter 7** **Data security and data storage**

### **Section 32** **Protection of information**

The registrar shall take the necessary technical and organizational measures to protect personal data against unauthorized access to data and to the accidental or unlawful destruction, alteration, transfer, transfer or other illegal processing of data. Measures should take into account the available technical possibilities, the cost of the measures, the quality, quantity and age of the data to be processed, and the importance of processing in terms of privacy.

Any person who acts as an independent trader on behalf of a controller shall, prior to the processing of data, give the controller appropriate commitments and otherwise adequate safeguards for the protection of personal data as referred to in subsection 1.

### **Section 33** **Obligation of confidentiality**

Any person who has knowledge of any other person's characteristics, personal circumstances or financial status when performing any processing of personal data may not, in violation of this Act, inform the other person of such information.

### **Section 34** **Disposal of an Identity Register**

The register of persons that is no longer necessary for the operations of the controller shall be destroyed unless the data stored therein are expressly provided or prescribed for retention, or if the register is not transferred to the repository referred to in section 35.

**Section 35****Transfer of personal data to the archive**

The use and protection of and the disclosure of personal data transferred to the National Archives Service or to a comparable archive shall be governed by what is specifically provided. However, the filing office or its comparable archive shall, when disclosing personal data from private individuals, take into account what is provided in this Act for the processing and disclosure of personal data unless it is obviously unnecessary for the privacy of the data subjects to take into account the age and quality of the data stored in the personal file.

An archive of a person who is relevant for scientific research or for any other reason may be transferred to a repository of an institution or authority carrying out a university or research activity as a statutory task if the National Archives has authorized it. The National Archives may authorize the Community, the Foundation and the institution to transfer to its archives personal registers created in their own operations that meet the above requirements. In its decision, the National Archives shall determine how protection of the registers should be organized and how the use of personal data should be monitored.

Before the authorization referred to in subsection 2. The National Archives must reserve an opportunity for the Data Protection Ombudsman to give an opinion.

**Chapter 8****Notice to the Data Protection Ombudsman****Section 36****The notification**

The registrar must report the automatic processing of personal data to the Data Protection Officer by submitting to this Privacy Policy.

In addition, the controller shall inform the Data Protection Ombudsman:

- 1) the transfer of personal data outside the territory of the Member States of the European Union or the European Economic Area if the data are transferred under Section 22 or under Section 23 or 6 or 7; mixed
- 2) the introduction of an automated decision-making system referred to in section 31.

Anyone who carries out credit information activities or is engaged in the pursuit of recovery or market research, or carries out tasks related to the selection and appraisal of personnel on behalf of another person, or in the processing and processing of personal registers and data in this activity is obliged to report to the Data Protection Officer.

If the processing of personal data is based on Section 8, subsection 1, paragraphs 1-3, paragraph 4, if the processing is regulated by law, the relationship or membership of a customer or service referred to in paragraph 5 or paragraphs 6 or 9 or Section 12 Paragraphs 1 to 4, 5, if the treatment is regulated by law, or paragraphs 7-10, 12 or 13, or 13-18 or 20. Furthermore, the obligation to notify may be waived, as provided for by regulation, if it is apparent that the processing of personal data does not infringe the privacy of the data subject or his rights or freedoms.

**Section 37****Make a notification**

The notification referred to in Section 36, subsection 2, paragraph 1 shall include, in addition to the information contained in the registration report, what data types are transferred and how the transfer takes place.

The notification referred to in Section 36, subsection 2. 2 point shall include the logic used in the system, in addition to the information contained in the registration report.

The notification referred to in Section 36, subsection 3. Should be disclosed the name, business, domicile and contact details of the business, the information registers used in the operation and the types of data contained therein, the possible disclosure of the data and the retention time of the data stored, how the protection of personal registers is organized and how their use is controlled.

The notification must be made in good time, but not later than 30 days before the personal data collected in the personal register are collected and deposited, or the filing of any other notification obligation.

## **Chapter 9**

### **Control and control of personal data processing**

#### **Section 38**

##### **Data protection authorities**

The EDPS provides guidance and advice on the processing of personal data and monitors the processing of personal data in order to implement the objectives of this Act and exercises the power of decision as provided in this Act.

The Data Protection Board deals with matters of principle concerning the processing of personal data related to the scope of the law and exercises decision-making power in data protection as provided by this law.

Data Protection Authorities may use the powers referred to in this Chapter even when the processing of personal data is not governed by this Law in accordance with Section 4. The data protection authorities cooperate with the data protection authorities of the other Member States of the European Union and provide, where appropriate, official assistance.

#### **Section 39**

##### **Data protection and inspection right of the data protection authorities**

The Data Protection Ombudsman is entitled, without prejudice to the confidentiality provisions, to obtain the information on the personal data processed and any information necessary for the lawfulness of the processing of personal data. The Data Protection Board has a similar right in its cases.

The Data Protection Ombudsman has the right to inspect the personal registers and to use experts in the audit. For the purposes of the audit, the Data Protection Officer and the expert have the right to access to such premises and personal property as well as to access the information and equipment necessary for the purpose of the inspection. In the space covered by the home page, the inspection may only be provided if, in the present case, there is an identified cause for suspicion of breach or breach of the provisions on the processing of personal data. The audit must be provided in such a way that it does not entail unnecessary harm to the controller and costs.

With regard to the processing referred to in section 2, subsection 5, the EDPS supervises compliance with the obligation to protect the information provided in section 32. The Data Protection Ombudsman is entitled, for this purpose, to obtain the necessary information about the protection of the registers.

#### **Section 40**

##### **Measures taken by the EDPS**

The EDPS should promote good computing, as well as guidance and advice, to ensure that the unlawful procedure is not resumed or renewed. Where appropriate, the Data Protection Supervisor shall bring the matter to the decision of the Data Protection Board or notify it for prosecution.

The Data Protection Ombudsman must resolve the matter that the registrar has filed under Article 28 and 29 for his consideration. The Data Protection Ombudsman may issue a controller with a record of enforcing the registered right of inspection or correcting the information.

The EDPS may provide more detailed guidance on how personal data should be protected against the unauthorized processing of personal data.

**Section 41****Hearing of the Data Protection Supervisor**

The relevant authority shall provide the Data Protection Ombudsman with an opportunity to be heard when preparing legislative or administrative reforms concerning the protection of the rights and freedoms of individuals with regard to the processing of personal data.

The Public Prosecutor shall be heard by the Data Protection Officer prior to the initiation of a prosecution against this Act. When dealing with such matters, the court has to give the Data Protection Ombudsman the opportunity to be heard.

**Section 42****Sectoral code of conduct**

Regulators or their representative bodies may establish sector-specific codes of conduct for the application of this Act and for the promotion of good computing, and submit proposals to the Data Protection Supervisor. The EDPS may check that the Code of Conduct complies with this Act and other provisions affecting the processing of personal data.

**Section 43****Privacy Protection Board**

The Data Protection Board may authorize the processing of personal data as referred to in section 8, subsection 1. 9, if processing is necessary to protect the data subject's vital interest in a non-individual case or to perform a public interest task or to exercise the public authority that belongs to the controller or third party to whom the data are disclosed. A permit may also be granted for the exercise of a legitimate interest of a controller or data subject, provided that such processing of data does not compromise the privacy and rights of the person.

The Data Protection Board may authorize the processing of sensitive personal data as referred to in section 12, paragraph 13, for important public interest reasons.

The authorization may be granted for a limited period or for an indefinite period and must be accompanied by the necessary provisions for the protection of the data subject's privacy. The provisions may, at the request of the Data Protection Officer or Authorizing Officer, be amended or supplemented if necessary due to changed circumstances.

**Section 44****Regulations of the Data Protection Board**

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

- 1) prohibit the processing of personal data contrary to this Act or to the provisions adopted pursuant thereto;
- (2) order, in matters other than those referred to in Paragraph 40 (2), within the relevant time limit to rectify what is wrongfully committed or negligent;
- 3) order the termination of registration activities if unlawful acts or omissions seriously undermine the protection of the data subject's privacy or his interests or rights, unless the register provides for the law; mixed
- 4) revoke the authorization referred to in section 43 when the conditions for granting the permit no longer exist or when the controller acts in contravention of the authorization or the provisions attached thereto.

**Section 45****Appeal**

Section 40, subsection 2. Of the Data Protection Supervisor and Section 43 and Section 44 of the Data Protection Board are appealed against by appealing in compliance with the provisions of Administrative

Instruction Act (586/1996). The Data Protection Supervisor may appeal to a decision of the Data Protection Board pursuant to Section 43.

The decision of the Data Protection Board may stipulate that a decision shall be enforced despite the appeal, unless otherwise ordered by the appeal authority.

#### **Section 46**

##### **Penalty payment**

The Data Protection Ombudsman may impose an obligation to provide information in accordance with Section 39, subsection 1 and Section 40, subsection 2. And the decision of the Data Protection Board pursuant to section 39 subsection 1. and the decision made pursuant to section 44 to impose the penalty as the penalty bill (1113/1990 ).

## **Chapter 10**

### **Various provisions**

#### **Section 47**

##### **Liability for damages**

The Registrar shall be liable for any financial and other damages incurred by the data subject or any other person against the processing of personal data against this Act.

Other damages are otherwise covered by Chapter 2, Sections 2 and 3, Chapter 3, Sections 4, 6 Sections and Chapters 4, 6 and 7 of the Damages Act (412/1974).

#### **Section 48**

##### **Penal provisions**

Penalty for a criminal record is provided in chapter 38, section 9 of the Criminal Code (39/1889) and in the personal data register in Chapter 38 Section 8 of the Criminal Code. Penalty for breach of the secrecy obligation provided for in section 33 shall be condemned in accordance with Chapter 38, sections 1 or 2 of the Criminal Code, unless the offense is punishable under Chapter 40, Section 5 of the Criminal Code, or otherwise punishable by a more severe punishment.

Any intentional or gross negligence in violation of this law

1) fails to comply with the provisions on the definition of the purpose of the processing of personal data, the filing of an inventory report, processing of data, informing him, correcting the information in the personal register, the denial of the registered right or making a notification to the Data Protection Officer;

2) give the Data Protection Authority incorrect or misleading information on the processing of personal data,

3. Violates the provisions on the protection of personal data and the destruction of personal data; or

4) violates the legally binding order issued by the Data Protection Board pursuant to section 43, subsection 3

and thus endanger the privacy or protection of his rights, shall be sentenced, unless the act is provided elsewhere in the law more severe penalty, *a personal data breach* to a fine.

#### **Section 49**

##### **Detailed provisions**

More detailed provisions on the implementation of this law are provided by decree.

## **Chapter 11**

### **Entry into force and transitional provisions**

#### **Section 50**

**Passage**

This law comes into force on 1 June 1999.

This Act repeals the Personal Register Law of 30 April 1987 (471/1987) with subsequent amendments. However, the provisions on the definitions of mass deployment and sensitive sampling of the repealed law will continue to apply, to the extent that other legislation refers to them, until 24 October 2001.

Measures enforcement of the law requires to be taken before the entry into force of this Act.

**Section 51  
transitional provisions**

The handling of personal data that has been initiated before the entry into force of this Act must bring the requirements of this Act into effect by 24 October 2001 at the latest.

If other legislation refers to the statute of the person or its provisions repealed by this Act, this reference shall be construed as referring to this Act or its corresponding provisions.

HE 96/1998 HAVM

26/1998

EV 278/1998

Helsinki on 22 April 1999

President of the Republic  
**MARTTI AHTISAARI**

Minister of Justice  
**Johannes Koskinen**

[Finlex](#) > [Legislation](#) > [Acts of origin](#) > [1999](#) > 523/1999

Finlex ® is a public and free Internet service provided by the Ministry of Justice.  
Finlex's content is produced and maintained by Edita Publishing Oy. The Ministry of Justice or Edita shall not be liable for errors that may arise in the contents of the databases, direct or indirect damage to the user's access, or interruptions or other interruptions in the Internet.