

Amendment:

2004-01-01 Journal of Laws of 2002 No. 153, item 1271 art. 52

2004-03-01 Journal of Laws No. 25, item 219 art. 181

**ACT**  
of August 29, 1997  
**on the Protection of Personal Data**

(original text - Journal of Laws of October 29, 1997, No. 133, item 883)  
(unified text – Journal of Laws of July 6, 2002, No. 101, item 926)

**CHAPTER 1**  
**General Provisions**

**Article 1**

1. Any person has a right to have his/her personal data protected.
2. The processing of personal data can be carried out in the public interest, the interest of the data subject, or the interest of any third party, within the scope and subject to the procedure provided for by the Act.

**Article 2**

1. The Act shall determine the principles of personal data processing and the rights of natural persons whose personal data is or can be processed as a part of a data filing system\*.
2. The Act shall apply to the processing of personal data in computer systems and other files, indexes, books, lists, and other registers.
3. With regard to the personal data files prepared *ad hoc*, exclusively for technical, training, or higher education purposes, where the data after being used are immediately removed or rendered anonymous, only the provisions of Chapter 5 shall apply.

**Article 3**

1. The Act shall apply to state authorities and territorial selfgovernment authorities, as well as to other state and municipal organisational units and non governmental bodies carrying out public tasks.
2. The Act shall also apply to natural and legal persons, and organisational units without the status of a legal person involved in the processing of data as a part of their business or professional activity or the implementation of statutory objectives.
3. The Act shall apply to the subjects referred to in paragraph 1 and 2 above having the seat or residing on the territory of the Republic of Poland, not having the seat or not residing on the territory of the Republic of Poland involved in the processing of data by means of technical devices located on the territory of the Republic of Poland.

4. The Act shall not apply to natural persons involved in the processing of data in the exercise of activities which are exclusively personal or domestic.

#### **Article 4**

The provisions of the Act shall apply, save where otherwise provided for by any international agreement to which the Republic of Poland is a party.

#### **Article 5**

Should the provisions of any separate laws on the processing of data provide for more effective protection of the data than the provisions hereof, the provisions of those laws shall apply.

#### **Article 6**

1. Within the meaning of the Act personal data shall mean any information relating to an identified or identifiable natural person.
2. An identifiable person is the one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
3. A piece of information shall not be regarded as identifiable where the identification requires an unreasonable amount of time, cost and manpower.

#### **Article 7**

Whenever in this Act a reference is made to any of the following, it shall mean:

1. data filing system - shall mean any structured set of personal data which are accessible pursuant to specific criteria, whether centralised, decentralised or dispersed on a functional basis,
2. processing of data - shall mean any operation which is performed upon personal data, such as collection, recording, storage, organisation, alteration, disclosure and erasure, and in particular those performed in the computer systems,
  - a) computer system - shall mean a set of co-operating devices, utilities, procedures of data processing and software tools which assist personal data processing,
  - b) security of data within computer systems – shall mean an implementation and usage of appropriate technical and administrative measures applied to protect data against unauthorized processing,
3. data erasure - shall mean destruction of personal data or such modification which would prevent determining the identity of the data subject,

4. controller - shall mean a body, an institution, an organisational unit, an establishment or a person referred to in Article 3.1 and 3.2 who decides on the purposes and means of the processing of personal data,
5. the data subject's consent - shall mean a declaration of will by which the data subject signifies his/her agreement to personal data relating to him/her being processed; the consent cannot be alleged or presumed on the basis of the declaration of will of other content.

## **CHAPTER 2**

### **Supervisory Authority for Personal Data Protection**

#### **Article 8**

1. The supervisory authority for the protection of personal data shall be the Inspector General for Personal Data Protection, hereinafter called "the Inspector General".
2. The Inspector General is appointed and dismissed by the Diet of the Republic of Poland with the consent of the Senate.
3. Only a person who meets inclusively the following requirements may be appointed to the position of the Inspector General:
  - 1) he/she is a Polish citizen permanently residing within the territory of the Republic of Poland,
  - 2) he/she is known for outstanding moral principles,
  - 3) he/she has a degree in law and a proper professional experience,
  - 4) he/she has no criminal record.
4. With regard to the performance of the duties entrusted to the Inspector General, he shall be solely subject to provisions governed by the Act.
5. The term of office of the Inspector General shall last 4 years following the date of his /her taking the oath. After the expiration of his/her term the Inspector General shall continue to perform his/her duties until the new Inspector General takes over his/her position.
6. The same person may hold the office of the Inspector General for not more than two terms.
7. The term of office of the Inspector General shall expire with his/her death; dismissal or the loss of the Polish citizenship.
8. The Diet, with the consent of the Senate shall dismiss the Inspector General, in case of:
  - 1) his/her resignation,
  - 2) becoming permanently unable to perform his/her duties due to an illness,
  - 3) violating his/her oath,
  - 4) being sentenced pursuant to a valid in law court judgement for committing a crime.

#### **Article 9**

Prior to assuming his/her duties, the Inspector General shall take the following oath before the Diet of the Republic of Poland:

"Assuming the post of the Inspector General for Personal Data Protection I hereby solemnly swear to observe the provisions of the Constitutional Act of the Republic of Poland, to safeguard the right for personal data protection, and to perform the duties entrusted to me conscientiously and impartially."

The oath may be taken with the words: "so help me, God".

#### **Article 10**

1. The Inspector General may neither hold another position except for a professor of a higher education institution nor perform any other professional duties.
2. The Inspector General may not be a member of any political party or any trade union, or be involved in any public activity which cannot be combined with the honour of the Inspector General's post.

#### **Article 11**

The Inspector General may neither be held criminally responsible or deprived of freedom without the prior consent of the Diet. The Inspector General may not be detained or arrested, except in *flagrante delicto*, and if his/her detention is necessary to secure the due course of proceedings. In such case the Speaker of the Diet has to be notified of the detention forthwith and may order the detainee to be immediately released.

#### **Article 12**

The duties entrusted to the Inspector General comprise, in particular:

- 1) supervision over ensuring the compliance of data processing with the provisions on the protection of personal data,
- 2) issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data,
- 3) keeping the register of data filing systems and providing information on the registered data files,
- 4) issuing opinions on bills and regulations with respect to the protection of personal data,
- 5) initiating and undertaking activities to improve the protection of personal data,
- 6) participating in the work of international organisations and institutions involved in personal data protection.

#### **Article 13**

1. The Inspector General shall perform his/her duties assisted by the Bureau of the Inspector General for Personal Data Protection, hereinafter referred to as "the Bureau".

2. The Inspector General and the employees of the Bureau, hereinafter referred to as "the inspectors", are obliged to provide protection to the information which constitute state or trade secrets, disclosed to them during any inspection of data processing activities.
3. The principles of organisation and functioning of the Bureau shall be determined in its statute, granted, by means of a regulation, by the President of the Republic of Poland.

#### **Article 14**

In order to carry out the tasks referred to in Article 12 (1) and 12 (2), the Inspector General, or inspectors authorised by him/her shall be empowered, in particular to:

- 1) enter, from 6 a.m. to 10 p.m., upon presentation of a document of personal authorisation and service identity card, any premises where the data filing systems are being kept and to perform necessary examination or other inspection activities to assess the compliance of the data processing activities with the Act,
- 2) demand written or oral explanations, and to summon and question any person if it is necessary to determine the actual state of things,
- 3) demand presentation of documents and any data directly related to the subject of the inspection,
- 4) demand access - for inspection purposes - to any devices, data carriers, and computer systems used for data processing,
- 5) commission expertise and opinions to be prepared.

#### **Article 15**

1. The head of the unit and any natural person acting as a controller of personal data subject to the inspection are obliged to enable the inspector to perform the inspection functions, and in particular with regard to the activities referred to in Article 14 (1) to (4).
2. The inspector performing the inspection of the data filing systems as mentioned in article 43 (1) (1a) is authorized to access to any file in which personal data are stored only by means of a duly authorized representative of the unit under inspection.

#### **Article 16**

1. The inspector who carries out the inspection shall prepare the official report of the inspection. One copy of such an official report shall be delivered to the controller subject to the inspection.
2. The official report shall be signed by the inspector and the controller subject to the inspection. The latter may apply for his/her justified objections and comments being included in the official report.
3. Should the controller subject to inspection refuse to sign the official report, the inspector shall make a relevant entry with regard to such refusal on the official report. Whereas the controller may, within 7 days, present his/her position in writing to the Inspector General.

### **Article 17**

1. Should the inspector, on the basis of inspection results, reveal any breach of the provisions on the protection of personal data, he/she shall request the Inspector General to apply the measures referred to in Article 18.
2. On the basis of the inspection findings, the inspector may demand that disciplinary proceedings or any other action provided for by law be instituted against persons guilty of the negligence and he/she be notified, within the prescribed time, about the outcomes of such proceedings and the appropriate actions taken.

### **Article 18**

1. Should the inspection reveal any breach of the provision on personal data protection, the Inspector General *ex officio* or following a motion of the data subject, shall order the controller by means of an administrative decision, to restore the proper legal state, and in particular:
  - 1) to remedy the negligence,
  - 2) to complete, update, correct, disclose, or not to disclose personal data,
  - 3) to apply additional measures protecting the collected personal data,
  - 4) to suspend the cross-border flow of personal data,
  - 5) to safeguard the data or to transfer them to other parties,
  - 6) to erase the personal data.
2. The Inspector General's decisions referred to in Article 18 (1) may not restrict the freedom of the subject which nominates candidates or submits lists of candidates for President of the Republic of Poland elections, elections to the Diet, the Senate and territorial selfgovernment bodies, as well as election to the European Parliament between the day when the election is announced and the voting day.
  - 2a. The Inspector General's decisions as mentioned in Article 18 (1), regarding the filing systems referred in article 43 (1) (1a), cannot order an erasure of personal data collected in inquiry activities carried out on a basis of legal provisions.
3. Should provisions of other laws regulate otherwise the performance of the actions referred to in Article 18.1, these provisions are applicable.

### **Article 19**

Should the inspection reveal that the action or failure in duties of the head of an organisational unit, its employee or any other natural person acting as the controller bears attributes of an offence within the meaning of the Act, the Inspector General shall inform about it a proper prosecuting body, enclosing the evidence confirming his/her suspicions.

### **Article 20**

Once a year the Inspector General shall submit to the Diet a report on his/her activities including conclusions with respect to observance of the provisions on personal data protection.

### **Article 21**

1. Any party may apply to the Inspector General for reconsidering its case.
2. The decision by the Inspector General on the application to reconsider the case may be appealed against with the administrative court.

### **Article 22**

The proceedings with respect to the matters regulated by this Act shall be conducted pursuant to the provisions of the Code of Administrative Procedure, unless other provisions of the law state otherwise.

## **CHAPTER 3**

### **The Principles of Personal Data Processing**

### **Article 23**

1. The processing of data is permitted only if:
  - 1) the data subject has given his/her consent, unless the processing consists in erasure of personal data,
  - 2) processing is provided for by law,
  - 3) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,
  - 4) processing is necessary for the performance of a task provided for by law and carried out in the public interest,
  - 5) processing is necessary for the purposes of the legitimate interests pursued by the controller referred to in Article 3 (2) or any third parties to whom the data are transferred, provided that the processing of the data does not violate the rights and the freedoms of the data subject.
2. The consent referred to in paragraph 1, point 1 may also be applied to future data processing, on the condition that the purpose of the processing remains unchanged.
3. Should the processing of data be necessary to protect the vital interests of the data subject and the condition referred to in paragraph 1, point 1 cannot be fulfilled, the data may be processed without the consent of the data subject until such consent can be obtained.
4. The legitimate interests, referred to in paragraph 1, point 5 in particular, are considered to be:
  - 1) direct marketing of own products or services provided by the controller,

2) vindication of claims resulting from economic activity.

#### **Article 24**

1. In cases, where personal data are collected from the data subject, the controller is obliged to provide a data subject from whom the data are collected with the following information:
  - 1) the address of its seat and its full name, and in case the controller is a natural person about the address of his/her residence and his/her full name,
  - 2) the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known at the date of collecting,
  - 3) the existence of the data subject's right of access and right to rectify the data concerning him/her,
  - 4) whether the replies to the questions are obligatory or voluntary, and in case of existence of the obligation about its legal basis.
2. The paragraph 1 does not apply if:
  - 1) any provision of other law allows for personal data processing without a disclosure of the real purpose for which the data are collected,
  - 2) the data subject already has the information referred to in paragraph 1.

#### **Article 25**

1. Where the data have not been obtained from the data subject, the controller is obliged to provide the data subject, immediately after the recording of his/her personal data, with the following information:
  - 1) the address of its seat and its full name, and in case the controller is a natural person about the address of his/her residence and his/her full name,
  - 2) the purpose and the scope of data collection, and in particular, about the data recipients or categories of recipients,
  - 3) the source of data,
  - 4) the existence of the data subject's right of access and right to rectify the data concerning him/her,
  - 5) the powers resulting from Article 32 (1) (7) and (8).
2. The provisions of paragraph 1 shall not apply where:
  - 1) the provision of other law provide or allow for personal data collection without the need to notify the data subject,
  - 2) the data to be collected are publicly available,
  - 3) the data are necessary for scientific, didactic, historical, statistic or public opinion research, the processing of such data does not violate the rights or freedoms of the data

subject, and the fulfilment of the terms and conditions determined by paragraph 1 would involve disproportionate efforts or endanger the success of the research,

- 4) the controller does not intend further processing of the collected data after single use,
- 5) data are processed by the controller as mentioned in Article 3 (1) by virtue of legal provisions,
- 6) the data subject already has the information referred to in paragraph 1.

#### **Article 26**

1. The controller performing the processing of data should protect the interests of data subjects with due care, and in particular to ensure that:
  - 1) the data are processed lawfully,
  - 2) the data are collected for specified and legitimate purposes and no further processed in a way incompatible with the intended purposes, subject to the provisions of paragraph 2 below,
  - 3) the data are relevant and adequate to the purposes for which they are processed,
  - 4) the data are kept in a form which permits identification of the data subjects no longer than it is necessary for the purposes for which they are processed.
2. The processing of data, for the purpose other than intended at the time of data collection is allowed provided that it does not violate the rights and freedoms of the data subject and is done:
  - 1) for the purposes of scientific, didactic, historical or statistical research,
  - 2) subject to the provisions of Article 23 and Article 25.

#### **Article 26a**

1. It is inadmissible whenever a final decision in an individual case of the data subject is to be issued if solely based on automated processing of personal data in a computer system.
2. The provision of paragraph 1 does not apply if the decision is taken in the course of entering into or performance of a contract and the request lodged by the data subject has been satisfied.

#### **Article 27**

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings shall be prohibited.
2. Processing of the data referred to in paragraph 1 above shall not constitute a breach of the act where:

- 1) the data subject has given his/her written consent, unless the processing consists in erasure of personal data,
- 2) the specific provisions of other statute provide for the processing of such data without the data subject's consent and provide for adequate safeguards,
- 3) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent until the establishing of a guardian or a curator,
- 4) processing is necessary for the purposes of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit-seeking organisations or institutions with a political, scientific, religious, philosophical, or trade-union aim and provided that the processing relates solely to the members of those organisations or institutions or to the persons who have a regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data,
- 5) processing relates to the data necessary to pursue a legal claim,
- 6) processing is necessary for the purposes of carrying out the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law,
- 7) processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards,
- 8) the processing relates to those data which were made publicly available by the data subject,
- 9) it is necessary to conduct scientific researches including preparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects,
- 10) data processing is conducted by a party to make the exercise of rights and duties resulting from decisions issued in court or administrative proceedings.

#### **Article 28**

1. Deleted
2. Serial numbers applied in the census may include only such features as: sex, date of birth, consecutive number, and control number.
3. Assigning any hidden meaning to the elements of serial numbers in the filing systems of data relating to natural persons shall be prohibited.

#### **Article 29**

1. In case of providing the access to the data for the purposes other than including into the data filing system, the controller referred to in Article 3 (1) shall disclose the data kept in the filing system to persons or subjects authorised by the law.

2. Personal data, exclusive of data referred to in Article 27 (1), may also be disclosed, for the purposes other than including into the data filing system, to persons and subjects other than those referred to in paragraph 1 above, provided that such persons or subjects present reliably their reasons for being granted the access to the data and that granting such access will not violate the rights and freedoms of the data subjects.
3. Personal data are disclosed at written and justified requests, unless the provisions of another law state otherwise. Such requests should include information allowing for identification the requested personal data within the filing system and indicating their scope and purpose.
4. Disclosed personal data shall be used only pursuant to the purpose for which they have been disclosed.

### **Article 30**

The controller shall refuse the access to the personal data of the filing system to subjects and persons other than those referred to in Article 29 (1), if it would:

- 1) result in the disclosure of the information constituting a state secrecy,
- 2) pose a threat to national defence or security of the state, human life and health, property, security and public order,
- 3) pose a threat to fundamental economic or financial interests of the state,
- 4) result in a substantial breach of personal interests of the data subjects or other persons.

### **Article 31**

1. The controller may authorise another subject to carry out the processing of personal data pursuant to a contract concluded in writing.
2. The subject, referred to in paragraph 1 above, may process the data solely within the scope and for the purpose determined in the contract.
3. The subject, referred to in paragraph 1, prior to processing the data shall be obliged to provide security measures protecting the data filing system, as defined in Articles 36 to 39.
4. In cases referred to in paragraphs 1 to 3, the liability for compliance with the provisions hereof, shall remain with the controller, whereas the contracting party shall not be exempted from the liability in case the data are processed in a way incompatible with the contract.

## **CHAPTER 4**

### **The Rights of the Data Subject**

### **Article 32**

1. The data subject has a right to control the processing of his/her personal data and contained in the filing systems, and in particular he has the right to:

- 1) obtain extensive information on whether such system exists and to establish the controller's identity, the address of its seat and its full name, and in case the controller is a natural person to obtain his/her address and his/her full name,
  - 2) obtain information as to the purpose, scope, and the means of processing of the data contained in the system,
  - 3) obtain information since when his/her personal data are being processed and communication to him/her in an intelligible form of the content of the data,
  - 4) obtain information as to the source of his/her personal data, unless the controller is obliged to keep it confidential as a state, trade or professional secret,
  - 5) obtain information about the means in which the data are disclosed, and in particular about the recipients or categories of recipients of the data,
  - 6) demand the data to be completed, updated, rectified, temporally or permanently suspended or erased, in case they are not complete, outdated, untrue or collected with the violation of the act, or in case they are no longer required for the purpose for which they have been collected,
  - 7) make a justified demand in writing, in cases referred to in Article 23 (1) (4) and (5), for the blocking of the data the processing of which has to be stopped, due to a particular situation,
  - 8) object against the processing of his/her personal data in cases referred to in Article 23 (1) (4) and (5), should the controller intend to process the data for marketing purposes or to object against the transfer of the data to another controller,
  - 9) make a demand to a controller for a judicial review of the case settled in contravention of article 26a (1).
2. In case of the demand referred to in paragraph 1(7) the controller shall immediately stop the processing of the questioned data or without undue delay transmit the demand to the Inspector General who shall make an appropriate decision.
  3. In case of the objection referred to in paragraph 1(8) further processing of the questioned data shall be prohibited. However, the controller is allowed to leave in filing system forename or forenames and a surname of a person with a PESEL identification number or address solely for the reason to avoid the data being used once more for the purposes to which the data subjects objected.
    - 3a. In case of the demand referred to in Article 32 (1) (9) the controller without undue delay shall consider the case or transmit it, together with his/her reasoned stand, to the Inspector General who shall issue an appropriate decision.
  4. In case where data processing is for scientific, didactic, historical, statistical or archival purposes the controller may not notify the data subject about the processing of his/her personal data, if the provision of such information involves disproportionate efforts.
  5. The concerned party may exercise his/her right of access to data referred to in paragraph 1 (1) to (5) once every six months.

### **Article 33**

1. At the request of the data subject, within the period of 30 days, the controller shall be obliged to notify the data subject about his/her rights, and in particular specify in an intelligible form:
  - 1) the category of personal data contained in the file,
  - 2) the means of data collection,
  - 3) the purpose and the scope of data processing,
  - 4) the recipients of the data and the scope of access they have been granted.
2. At the request of the data subject, the information referred to in paragraph 1 shall be given in writing.

### **Article 34**

The provisions of Article 30 shall apply in all matters related to notification and disclosure of the data to the data subject.

### **Article 35**

1. Should the data subject prove that the personal data relating to him/her are not complete, they are outdated, untrue or collected with the violation of the act, or in case they are no longer required for the purpose for which they have been collected, the controller shall be obliged, without undue delay, to amend, update, or correct the data, or to temporarily or permanently suspend the processing of the questioned data, or to have them erased from the filing system, unless the above refers to the personal data which shall be amended, updated or corrected pursuant to the principles determined by other laws.
2. Should the controller fail to fulfil the obligation referred to in paragraph 1 above, the data subject may apply to the Inspector General to issue a relevant order to the controller.
3. The controller shall be obliged without undue delay to inform other controllers, to whom he/she disclosed a data file, that some data have been updated or corrected.

## **CHAPTER 5**

### **Protection of Personal Data Filing Systems**

### **Article 36**

The controller shall be obliged to implement appropriate technical and organizational measures to protect the processed personal data, and in particular to protect personal data against their unauthorized disclosure, unauthorized takeover person, processing with the violation of the Act, any change, removal, damage or destruction.

### **Article 37**

The computer system and devices constituting the system used for the processing of data shall be operated solely by persons authorised by the controller.

#### **Article 38**

The controller of the data processed in computer systems shall control the category of personal data entered into the system and also the dates of such entry, the entering persons, and the recipients of the data, in particular where the data is transferred by means of telecommunications services.

#### **Article 39**

1. The controller shall keep the register of persons involved in the processing of personal data.
2. The persons referred to in paragraph 1 above, who have the access to personal data, shall be obliged to keep them confidential. The obligation remains in force after the termination of their employment contract.

### **CHAPTER 6**

#### **Registration of Personal Data Filing Systems**

#### **Article 40**

The controller shall be obliged to register a data filing system with the Inspector General. The above shall not apply in cases referred to in Article 43 (1).

#### **Article 41**

1. The notification, concerning the data filing system submitted to the registration, should contain the following:
  - 1) an application for entering the personal data filing system into the register of filing systems,
  - 2) an indication of the controller and the address of its seat or place of residence, including the identification number in the register of enterprises setting up in business, if applicable, and the legal grounds on which he/she is authorised to run the data filing system,
  - 3) the scope and purpose of the personal data processing,
  - 4) information on the ways and means of data collection and disclosure,
    - 4a) information upon the recipients or categories of recipients to whom the data may be transferred,
  - 5) the description of technical and organisational measures applied for the purposes referred to in Article 36 to 39,
  - 6) information on the ways and means of fulfilling technical and organisational requirements referred to in Article 45 (1),

- 7) information referring to an optional, international transfer of data.
2. The controller shall be obliged to notify the Inspector General about any changes affecting the information referred to in Article 41 (1) within 30 days following the date of the change introduced to the filing system.\*

#### **Article 42**

1. The Inspector General shall keep a national open register of personal data filing systems submitted to registration. The register should contain information listed in Article 41 (1).
2. The register referred to in paragraph 1 may be inspected by any person.
3. At the request, the concerned party may obtain the certificate of registration of the filing system.

#### **Article 43**

1. The obligation to register filing systems shall not apply to the controllers of such data which:
  - 1) constitute a state secrecy due to the reasons of state defence or security, human life and health, property, security, or public order,
    - 1a) were collected as a result of inquiry procedures held by officers of the bodies authorized to conduct such inquiries,
  - 2) are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on National Criminal Register,
    - 2a) are processed by the Inspector General of Financial Information,
  - 3) relating to the members of churches or religious unions with an established legal status,
  - 4) refer to the persons employed by them, their members or trainees,
  - 5) refer to the persons availing themselves of their health care services, notarial or legal advice, patent agent, tax consultant or auditor services,
  - 6) are created on the basis of electoral regulations concerning the Diet, Senate, European Parliament, communal councils, poviats councils and voivodship regional councils, the President of the Republic of Poland, head of the commune, mayor or president of a city elections, and the acts on referendum and municipal referendum,
  - 7) refer to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom,
  - 8) are processed for the purpose of issuing an invoice or for accounting purposes,
  - 9) are publicly available,
  - 10) are processed to prepare a thesis required to graduate from a university or be granted a degree,
  - 11) are processed with regard to current everyday affairs.
2. As regards data filing systems referred to in Article 43 (1) (1) and (3) and those referred to in Article 43(1)(1a) processed by state security offices within the meaning of the Act of January 22, 1999 on the protection of classified information (O.J., No. 11, item 95, of 2000, No.12,

item 136 and No. 39, item 462 and of 2001, No. 22, item 247 and No. 27, item 298) the Inspector General is not entitled to the powers stipulated in Article 12 (2) and Article 14(1), (3) to (5) and articles 15 to 18.

#### **Article 44**

1. The Inspector General shall, by means of an administrative decision refuse to register the data filing system if:
  - 1) the requirements specified in Article 41 (1) have not been fulfilled,
  - 2) the processing may violate the provisions provided for by Articles 23 to 30,
  - 3) the devices and computer systems, used for processing of the datafiling system submitted for registration, do not meet fundamental technical and organisational conditions defined in Article 45 (1).
2. Should the Inspector General refuse to register a data filing system, he/she shall order the suspension of further data processing in this filing system or the erasure of the data.
3. The order to suspend further data processing or to erase the data shall be enforced immediately.
4. After the removal of the defects which resulted in the refusal to register any data filing system, the controller may again submit the system for registration.
5. Should a data filing system be re-submitted for the registration, the controller may start the processing of data after its registration.

#### **Article 45**

The Minister who is responsible for administrative matters, by way of a regulation, shall determine:

- 1) fundamental technical and organisational requirements for the devices and systems of automatic processing of personal data,
- 2) the form of an application referred to in Article 29 (3),
- 3) the form of a notification referred to in Article 41 (1),
- 4) the form of an authorisation and a service identity card referred to in Article 14 (1).

#### **Article 46**

The controller may start the processing of data in the data filing system after notification of the system to the Inspector General unless the controller is exempted from this obligation.

### **CHAPTER 7**

#### **Transborder Data Flows**

### **Article 47**

1. Any transfer of personal data across national borders shall take place only if a country of destination ensures at least the same level of personal data protection as that in force in the territory of the Republic of Poland.
2. The provision of paragraph 1 above shall not apply to the transfer of personal data required by other laws or by the provisions of any ratified international agreement.
3. Nevertheless the controller may transfer the personal data across national borders provided that:
  - 1) the data subject has given his/her written consent,
  - 2) the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request,
  - 3) the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and third party,
  - 4) the transfer is necessary or required by reasons of public interests or for the establishment of legal claims,
  - 5) the transfer is necessary in order to protect the vital interests of the data subject,
  - 6) the transfer relates to data which are publicly available.

### **Article 48**

In cases other than those referred to in Article 47(2) and (3) the transfer of personal data across national borders, to a country which does not ensure at least the same level of protection as that in force in the territory of the Republic of Poland, shall take place subject to a prior consent of the Inspector General.

## **CHAPTER 8**

### **Sanctions**

### **Article 49**

1. A person, who processes personal data in a data filing system where such processing is forbidden or where he is not authorised to carry out such processing, shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to two years.
2. Where the offence mentioned at point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to three years.

### **Article 50**

A person who, being the controller of a data filing system, stores personal data incompatible with the intended purpose for which the system has been created, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

### **Article 51**

1. A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorised persons, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to two years.
2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

### **Article 52**

A person who, being the controller of a data filing system violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised access, damage or destruction, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

### **Article 53**

A person who, regardless of the obligation, fails to notify of the data filing system for registration, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

### **Article 54**

A person who, being the controller, fails to inform the party to which the data relates, of its rights or of information which would enable that person to benefit from the provisions of this Act, is liable to a fine, partial restriction of freedom or prison sentence of up to one year.

## **CHAPTER 9**

### **Amendments to the Binding Regulations, Temporary Provisions, and Final Provisions**

### **Article 55**

In Article 2 (2) of the Act of July 30, 1981 on the remuneration of persons holding management posts in state administration (Journal of Laws No. 20, item 101; of 1982 No. 31, item 214; of 1985 No. 22, item 98, and No. 50, item 262; of 1987 No. 21, item 123; of 1989 No. 34, item 178; of 1991 No. 100, item 443; of 1993 No.1, item 1; of 1995 No. 34, item 163, and No.142, item 701; of 1996 No. 73, item 350, No. 89, item 402, No.106, item 496, and No. 139, item 647) after

the words "Commissioner for Citizens' Rights Protection" the words "The Inspector General for Personal Data Protection" shall be added.

#### **Article 56**

The Act of September 16, 1982 on the employees of state administration (Journal of Laws No. 31, item 214; of 1984 No. 35, item 187; of 1988 No.19, item 132; of 1989 No. 4, item 24, No. 34, item 178 and 182; of 1990 No. 20, item 121; of 1991 No. 55, item 234, No. 88, item 400, and No. 95, item 425; of 1992 No. 54, item 254, and No. 90, item 451; of 1994 No.136, item 704; of 1995; No 132, item 640; and of 1996 No. 89, item 402, and No.106, item 496) shall be altered as follows:

- 1) In Article 1, the following paragraph 13 shall be added: "in the Bureau of The Inspector General for Personal Data Protection";
- 2) In Article 36 (5) (1) the word "and" shall be replaced with a comma and after the words "The National Electoral Office" the following shall be added "the Bureau of the Inspector General for Personal Data Protection";
- 3) In Article 48 (1) (1) after the words "The Bureau of Commissioner for Citizens' Rights Protection" the following words shall be added "The Bureau of the Inspector General for Personal Data Protection".

#### **Article 57**

In Article 31(3) (2) of the Act of January 5, 1991 - the Budgetary Law (Journal of Laws of 1993 No. 72, item 344; of 1994 No. 76, item 344, No. 121, item 591, and No.133, item 685; of 1995 No. 78, item 390, No.124, item 601, and No.132, item 640; of 1996 No. 89, item 402, No.106, item 496, No. 132, item 621, and No.139, item 647; and of 1997 No. 54, item 348), after the words "the Supreme Chamber of Control" the following words shall be added "The Inspector General for Personal Data Protection".

#### **Article 58**

The Article 4 of the Act of December 23, 1994 on the Supreme Chamber of Control (Journal of Laws of 1995 No. 13, item 59, and of 1996 No. 64, item 315 and No. 89, item 402; and of 1997 No. 28, item 153) shall be altered as follows:

- 1) In paragraph 1 after the words "The National Broadcasting Council" the words " the Inspector General for Personal Data Protection" shall be added.;
- 2) In paragraph 2 after the words "The National Broadcasting Council" a comma and the words "the Inspector General for Personal Data Protection" shall be added.

#### **Article 59**

In Article 2 (2) of the Act of December 23, 1994 on the measures allocated to the state budgetary sector remuneration and on amendments to certain laws (Journal of Laws of 1995 No. 34, item 163 and of 1996 No. 106, item 496 and No. 139, item 647) after the words "The

National Electoral Office" the words "the Inspector General for Personal Data Protection" shall be added.

#### **Article 60**

In the Act of April 26, 1996 on the Prison Service (Journal of Laws No. 61, item 283 and No. 106, item 496, and of 1997 No. 28, item 153) the following Article 23(a) shall be added: Article 23a The Prison Service may collect and process information and personal data, also without the consent of the data subject, necessary to perform tasks referred to in Article 1(3) of the law."

#### **Article 61**

1. Parties referred to in Article 3, being on the date of entry into force of the Act the controllers of personal data automatic filing systems, shall be obliged to file an application for registration of the systems pursuant to the provisions of Article 41, within the period of 18 months of the date of entry into force of the Act, unless they are released from this obligation by virtue of law.
2. Until the personal data filing systems are registered pursuant to the provisions of Article 41, the subjects referred to in paragraph 1 may operate the systems without the registration.

#### **Article 62**

The Act shall enter into force after 6 months from the date of its publication, with the exclusion of:

- 1) Article 8 to 11, Article 13 and Article 45 which enter into force after 2 months from the date of publication,
- 2) Article 55 to 59 which enter into force after 14 days from the date of publication.

\* For the purpose of the Polish Act on the Personal Data Protection of August 29, 1997 a phrase "a data file – zbiór danych" is used as definitions of "a data filing system" and "a data file" remain the same.