

## Amendments

- 2004-01-01 Journal of Laws of 2002 No. 153, item 1271, Art. 52
- 2004-03-01 Journal of Laws of 2004 No. 25, item 219, Art. 181
- 2004-05-01 Journal of Laws of 2004 No. 33, item 285, Art. 1
- 2006-07-24 Journal of Laws of 2006 No. 104, item 708, Art. 178
- 2006-10-01 Journal of Laws of 2006 No. 104, item 711, Art. 31
- 2007-09-14 Journal of Laws of 2007 No. 165, item 1170, Art. 39
- 2007-10-10 Journal of Laws of 2007, No. 176, item 1238, Art. 13

## **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:
  - 1) files, indexes, books, lists and other registers,
  - 2) computer systems, also in case where data are processed outside from a data filing system.
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, territorial self-government authorities, as well as to state and municipal organisational units.
2. The Act shall also apply to:
  - 1) non-public bodies carrying out public tasks,
  - 2) natural and legal persons and organisational units not being legal persons, if they are involved in the processing of personal data as a part of their business or professional activity or the implementation of statutory objectives

- having the seat or residing in the territory of the Republic of Poland or in a third country, if they are involved in the processing of personal data by means of technical devices located in the territory of the Republic of Poland.

### **Article 3a**

1. The Act shall not apply to :
  - 1) natural persons involved in the processing of data for personal or domestic purposes exclusively,
  - 2) subjects having the seat or residing in a third country, making use of technical devices located in the territory of the Republic of Poland for the transfer of data exclusively.
2. Except for the provisions of Art. 14-19 and Art. 36 paragraph 1, the Act shall also not apply to press journalistic activity within the meaning of the Act of January 26, 1984 – Press Law (Journal of Laws No. 5, item 24, with later amendments) and literary and artistic activity, unless the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject.

### **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/her physical, physiological, mental, economic, cultural or social identity.
3. A piece of information shall not be regarded as identifying 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,
- 2a) computer system - shall mean a set of co-operating devices, utilities, procedures of data processing and software tools which are applied for the purpose of personal data processing,

- 2b) security of data within computer systems - shall mean an implementation and usage of appropriate technical and organisational 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 organisational unit, an establishment or a person referred to in Article 3, 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,
- 6) data recipient - shall mean any person to whom the data are disclosed, exclusive of:
  - a) the data subject,
  - b) a person authorised to carry out data processing,
  - c) a representative referred to in Article 31a,
  - d) a subject referred to in Article 31,
  - e) state authorities or territorial self-government authorities to whom the data are disclosed in connection with the proceedings conducted,
- 7) third country - shall mean a country which does not belong to the European Economic Area.

## **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/she shall be solely subject to the 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 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 Constitution 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 12a**

1. Upon a motion of the Inspector General, the Speaker of the Diet may appoint a Deputy Inspector General. The Deputy Inspector General is dismissed under the same procedure.
2. The Inspector General shall determine the scope of tasks of his/her deputy.
3. The Deputy Inspector General shall meet the requirements specified in Art. 8 paragraph 3 point 1, 2 and 4, and have higher education and a proper professional experience.

### **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. Deleted
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 point 1 and 2, the Inspector General, the Deputy Inspector General or employees of the Bureau, hereinafter referred to as "the 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 premises where data are processed outside from the data filing system, 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 within the scope necessary to determine the facts of the case,
- 3) consult any documents and data directly related to the subject of the inspection, and to make a copy of these documents,
- 4) perform inspection of 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 to perform the activities and meet the requirements referred to in Article 14 point 1 to 4.
2. The inspector performing the inspection of the data filing systems as mentioned in article 43 paragraph 1 point 1a is authorized to consult 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. In case of any breach of the provisions on personal data protection, the Inspector General ex officio or upon a motion of a person concerned, by means of an administrative decision, shall order 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 flow of personal data to a third country,
  - 5) to safeguard the data or to transfer them to other subjects,
  - 6) to erase the personal data.
2. The Inspector General's decisions referred to in Article 18 paragraph 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 self-government 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 paragraph 1, regarding the filing systems referred to in article 43 paragraph 1 point 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 paragraph 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.

## **Article 22a**

The minister who is responsible for public administration matters shall determine, by way of a regulation, the form of an authorization and a service identity card referred to in Article 14 point 1, considering the need for personal indication of an inspector employed in the Bureau of the Inspector General for Personal Data Protection.

## **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 necessary for the purpose of exercise of rights and duties resulting from a legal provision,
  - 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 tasks provided for by law and carried out in the public interest,
  - 5) processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and 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 case 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 to his/her data and the right to rectify these data,
  - 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 shall 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. In case 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 to his/her data and the right to rectify these data,
  - 5) the powers resulting from Article 32 paragraph 1 point 7 and 8.
2. The provisions of paragraph 1 shall not apply where:
  - 1) the provision of other law provides or allows for personal data collection without the need to notify the data subject,
  - 2) deleted,
  - 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) deleted,
  - 5) the data are processed by the controller referred to in Article 3 paragraph 1 and Article 3 paragraph 2 point 1 on the basis 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 exercise the 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 shall disclose the data kept in the data filing system to persons or subjects authorised by the law.
2. Personal data, exclusive of data referred to in Article 27 paragraph 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 of 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 paragraph 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, or 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 – 39, and to meet the requirements specified in the provisions referred to in Article 39a. With regard to the observance of these provisions the data subject shall bear the liability as the controller.
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.

5. The provisions of Articles 14 – 19 shall apply respectively to supervision over ensuring the compliance of data processing conducted by the subject referred to in paragraph 1 with the provisions on the protection of personal data.

#### **Article 31a**

In case of the processing of personal data by the subjects having the seat or residing in a third country, the controller shall be obliged to appoint its representative in the Republic of Poland.

### **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 contained in the filing systems, and in particular he/she 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 secrecy,
  - 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,
  - 5a) obtain information about the prerequisites of taking the decision referred to in Article 26a paragraph 2,
  - 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 paragraph 1 point 4 and 5, for the blocking of the processing of his/her data, due to his/her particular situation,
  - 8) object to the processing of his/her personal data in cases referred to in Article 23 paragraph 1 point 4 and 5, should the controller intend to process the data for marketing purposes or to object to the transfer of the data to another controller,
  - 9) make a demand to a controller for reconsidering of the individual case settled in contravention of article 26a paragraph 1.
2. In case of the demand referred to in paragraph 1 point 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 point 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 paragraph 1 point 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 to obtain information referred to in paragraph 1 point 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 provide him/her with the information referred to in Article 32 paragraph 1 point 1-5a as regards his/her personal data, 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 to inform without undue delay other controllers, to whom he/she disclosed a data file, that some data have been updated or corrected.

### **CHAPTER 5 Protection of Personal Data**

#### **Article 36**

1. The controller shall be obliged to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular to protect data against their unauthorised disclosure,

takeover by an unauthorised person, processing with the violation of the Act, any change, loss, damage or destruction.

2. The controller shall keep the documentation describing the way of data processing and measures referred to in paragraph 1.
3. The controller shall appoint an administrator of information security who supervises the compliance with security principles referred to in paragraph 1, unless the controller performs these activities by himself.

### **Article 37**

Exclusively persons who were granted an authorisation by the controller shall be allowed to carry out the processing of data.

### **Article 38**

The controller shall be obliged to ensure supervision over the following: which data, when and by whom have been entered into the filing system and to whom they are transferred.

### **Article 39**

1. The controller shall keep the register of persons authorised to carry out the processing of data, which should contain the following:
  - 1) full name of the authorised person,
  - 2) date of granting and expiring, as well as the scope of an authorisation to access personal data,
  - 3) identifier, in case where data are processed in a computer system,
2. The persons authorised to carry out the processing of data shall be obliged to keep these personal data and the ways of their protection confidential.

### **Article 39a**

The minister responsible for public administration matters in consultation with the minister responsible for informatisation shall determine, by way of a regulation, a way of keeping and scope of documentation referred to in Article 36 paragraph 2, as well as basic technical and organisational conditions which should be fulfilled by devices and computer systems used for the processing of personal data, considering ensuring the protection appropriate to the risks and category of data being protected, as well as the requirements with regard to keeping record of disclosure of personal data and security of the processed data.

## **CHAPTER 6**

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

### **Article 40**

The controller shall be obliged to notify a data filing system to registration by the Inspector General. The above shall not apply in cases referred to in Article 43 paragraph 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 subject running the filing system 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, and in case of the subject referred to in Article 31a, indication of this subject and the address of its seat or place of residence,
  - 3) the purpose of the processing of data,
  - 3a) description of the categories of data subjects and the scope of the processed data,
  - 4) information on the ways and means of data collection and disclosure,
  - 4a) information on 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 conditions specified in the provisions referred to in Article 39a,
  - 7) information relating to a possible data transfer to a third country.
2. The controller shall be obliged to notify the Inspector General about any changes affecting the information referred to in paragraph 1, within 30 days following the date of the change introduced to the filing system. The provisions on registration of personal data filing systems shall apply respectively to the notification about changes.

## **Article 42**

1. The Inspector General shall keep a national, open register of personal data filing systems. The register should contain the information referred to in Article 41 paragraph 1 point 1 – 4a and point 7.
2. The register referred to in paragraph 1 may be inspected by any person.
3. At the request, the controller may obtain the certificate of registration of data filing system notified by the controller, subject to the provisions of paragraph 4.
4. The Inspector General shall issue to the controller referred to in Article 27 paragraph 1 the certificate of registration of data filing system immediately after the registration.

## **Article 43**

1. The obligation to register data 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, protection of 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,
  - 2b) are processed by relevant bodies for the purposes of the participation of the Republic of Poland in the Schengen Information System and the Visa Information System,

- 3) relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions,
  - 4) are processed in connection with the employment by the controller or providing services for the controller on the grounds of civil law contracts, and also refer to the controller's members and 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, a bill 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 minor current everyday affairs.
2. As regards data filing systems referred to in Article 43 paragraph 1 point 1 and 3 and those referred to in Article 43 paragraph 1 point 1a processed by Internal Security Agency, Foreign Intelligence Agency, Central Anticorruption Bureau and Military Information Services the Inspector General is not entitled to the powers stipulated in Article 12 point 2 and Article 14 point 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 paragraph 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 the processing of the data filing system submitted for registration do not meet fundamental technical and organisational conditions defined in Article 39a.
2. Should the Inspector General refuse to register a data filing system, he/she shall order by means of an administrative decision to:
  - 1) limit the processing of all categories or some categories of data only to the storage of data, or
  - 2) apply other measures referred to in Article 18 paragraph 1.
3. Deleted.
4. After the removal of the defects which resulted in the refusal to register a 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 44a**

Striking off an entry in the register of the data filing systems shall be done by means of an administrative decision, in case where:

- 1) the data are no longer processed in the registered filing system,
- 2) the registration has been made with the violation of the law,

## **Article 45**

Deleted.

## **Article 46**

1. The controller may, subject to the provision of paragraph 2, 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 by virtue of the Act.
2. The controller of data referred to in Article 27 paragraph 1 may start the processing of these data in the data filing system after registration of the file, unless the controller is exempted from the obligation to submit the system for registration by virtue of the Act.

## **Article 46a**

The minister who is responsible for public administration matters shall determine, by way of a regulation, the form of a notification referred to in Article 41 paragraph 1, considering the obligation to include the information necessary to confirm the compliance of data processing with the requirements of the Act.

## **CHAPTER 7**

### **Transfer of Personal Data to a Third Country.**

## **Article 47**

1. The transfer of personal data to a third country may take place only, if the country of destination ensures at least the same level of personal data protection in its territory 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 legal provisions or by the provisions of any ratified international agreement.
3. Nevertheless the controller may transfer the personal data to a third country 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 another subject,
  - 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 paragraph 2 and 3 the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as that in force in the territory of the Republic of Poland, may take place subject to a prior consent of the Inspector General, provided that the controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject.

## **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/she 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 in 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 incompatibly 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 takeover, 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 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 data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be 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**

Ommited.

**Article 56**

Ommited.

**Article 57**

Ommited.

**Article 58**

Ommited.

**Article 59**

Ommited.

**Article 60**

Ommited.

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