

**THE REGULATION OF APRIL 29, 2004
BY THE MINISTER OF INTERNAL AFFAIRS AND ADMINISTRATION
As regards personal data processing documentation and technical and organisational
conditions which should be fulfilled by devices and computer systems used for the
personal data processing.**

Pursuant to Art. 39a of the Act of August 29, 1997 on Personal Data Protection (Journal of Laws of 2002, No. 101, item 926, No 153, item 1271 and of 2004, No. 25, item 219, No. 33, item 285) the following provisions have been adopted:

§ 1.

The Regulation shall determine:

- 1) the way and the scope in which documentation describing personal data processing is to be kept and technical and organisational measures providing the protection of the personal data being processed, appropriate to any danger and categories of protected data;
- 2) basic, technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing;
- 3) requirements as regards the recording of any personal data disclosure and security of personal data processing.

§ 2.

Whenever in this Regulation the reference is made to:

- 1) “the Act” shall mean the Act of August 29, 1997 on the Personal Data Protection, hereinafter called “the Act”;
- 2) “identifier of a user” shall mean the sequence of alpha-numerical or other signs which unambiguously identifies the person authorised to process personal data within the computer system;
- 3) “password” shall mean the sequence of alpha-numerical or other signs, known only to the person authorised to operate within computer system.

- 4) “telecommunications network” shall mean a telecommunications network within the meaning of Art. 2 point 23 of the Act of July 21, 2001 – Telecommunications Law (Journal of Laws No. 73, item 852, with later amendments);
- 5) “public network” shall mean a public network within the meaning of Art. 2 point 22 of the Act of July 21, 2001 – Telecommunications Law;
- 6) “transmission” shall mean a transmission of information over the telecommunications network;
- 7) “accountability” shall mean a feature ensuring that any action performed by given subject may be unambiguously attributed only to this subject;
- 8) “data integrity” shall mean a feature ensuring that personal data have not been changed or destroyed in unauthorised manner;
- 9) “report” shall mean lists concerning the scope and the content of processed, data drawn up by the computer system;
- 10) “data confidentiality” shall mean a feature ensuring that data are not disclosed to unauthorised subjects;
- 11) “authorisation” shall mean an action performed in order to verify subject’s claimed identity.

§ 3.

1. Documentation referred to in § 1 point 1 shall comprise of the security policy and the computer system management instruction used for personal data processing, hereinafter called “the instruction”.
2. Documentation referred to in § 1 point 1 shall be kept in writing.
3. Documentation referred to in § 1 point 1 shall be implemented by a controller.

§ 4.

The security policy referred to in § 3 paragraph 1 shall include in particular:

- 1) a list of buildings, premises or their parts comprising the area where the personal data are processed;
- 2) a list of data filing systems with an indication of software used for data processing;
- 3) a description of the structure of data filing systems and indication of the contents of particular information fields and connections between them;
- 4) method of transferring data between particular systems;
- 5) definition of technical and organisational measures necessary to ensure confidentiality, integrity and accountability of the data being processed.

§ 5.

The instruction referred to in § 3 paragraph 1 shall comprise in particular:

- 1) procedures of granting authorisation to process data and registration of these authorisations in the computer system as well as indication of the person responsible for the aforesaid activities;
- 2) applied methods and means of authorisation and procedures connected with their management and use;
- 3) procedures of the beginning, suspension and the end of work by the users of the system;
- 4) procedures of making back ups of the data filing systems and programs and software tools used for the data processing.
- 5) method, place and period of storage of:
 - a) electronic information media containing personal data,
 - b) back ups referred to in point 4,
- 6) method of the computer system securing against software referred to in paragraph III point 1 of the Appendix to this Regulation;
- 7) method of implementation of the requirements referred to in § 7 paragraph 1 point 4;
- 8) procedures of executing the inspection and maintenance of systems and information media used for personal data processing.

§ 6.

1. Having regard to the categories of data being processed and the dangers, the following security levels of personal data processing within the computer system shall be introduced:
 - 1) basic security level;
 - 2) medium security level;
 - 3) high security level.
2. At least the basic security level shall be applied if:
 - 1) data referred to in Art. 27 of the Act are not being processed within the computer system, and
 - 2) none of the computer system devices used for personal data processing is connected to the public network.
3. At least medium security level shall be applied if:

- 1) data referred to in Art. 27 are processed within the computer system, and
 - 2) none of the computer system devices used for personal data processing is connected to the public network.
4. High security level shall be applied if at least one of the computer system devices used for personal data processing is connected to the public network.
 5. Description of security measures applied on levels referred to in paragraph 1 shall be provided for by the Appendix to the Regulation.

§ 7.

1. For each person whose personal data are being processed within the computer system, except for the systems used for personal data processing which is limited solely to edition of the text in order to disclose this text in writing, that system should secure keeping records of:
 - 1) the date when the data have been registered for the first time in the system;
 - 2) an identifier of a user who registers the personal data in the system, unless the access to the computer system and personal data being processed within this system is available for one person only;
 - 3) data sources, in case where the data have not been obtained from data subject;
 - 4) information on recipients within the meaning of Art. 7 point 6 of the Act to whom the data have been disclosed and the date and the scope of this disclosure, unless the computer system is used for the processing of personal data contained in open data filing systems;
 - 5) an objection referred to in Art. 32 paragraph 1 point 8.
2. Keeping records of information referred to in paragraph 1 point 1 and 2 shall ensue automatically after the user's confirmation of the data recording.
3. The computer system used for personal data processing shall provide for the preparing and printing of the report, in an intelligible form, including information referred to in paragraph 1.
4. Where the personal data are processed in at least two computer systems, the requirements referred to in paragraph 1 point 4 may be implemented in one of them or in separate information system intended for this purpose.

§ 8.

The computer system used for personal data processing which has been admitted to the processing of classified information by the competent state security service after obtaining the

certificate issued under the provision of the Act on January 22, 1999 on the protection of classified information (Journal of Laws No. 11, item 95, with later amendments) fulfils the requirements of high security level provided for by this Regulation.

§ 9.

The controller of personal data being processed on the day this Regulation comes into force shall be obliged to adjust the computer systems used for personal data processing to the requirements provided for by § 7 and Appendix to this Regulation within the period of 6 months of the effective date of this Regulation.

§ 10.

The Regulation shall enter into force on the day the Republic of Poland becomes a member of the European Union.

Appendix to the Regulation of April 29, 2004 (item. 1024) by the Minister of Internal Affairs and Administration.

A. Security measures at the basic security level

I

1. The area referred to in § 4 point 1 of the Regulation shall be secured against access of unauthorised persons during the absence in this area of the persons authorised to process personal data.
2. Any unauthorised person may stay inside the area referred to in § 4 point 1 of the Regulation only by the controller's consent or in the presence of a person authorised to process personal data.

II

1. The access control mechanisms shall be applied in the computer system used for personal data processing.
2. If the access to data being processed in the computer system is granted to at least two persons the following conditions shall be ensured that:
 - a) a separate identifier shall be registered for each user of the computer system;
 - b) access to data is available only after entering the identifier and user's authentication.

III

The computer system used for personal data processing shall be secured in particular against:

- 1) software used for gaining unauthorised access to the computer system;
- 2) loss of data which may be caused by any power supply failure or line interference.

IV

1. The identifier of a user who has lost authorisation to personal data processing should not be granted to other person.
2. In case where the password is used for user authentication, the passwords shall be changed at least once a month. The password consists of at least 6 characters.
3. Personal data being processed within the computer system shall be secured by making of back ups of the data filing systems and using of data processing software.
4. Back ups should:
 - a) be stored in the premises ensuring security against any unauthorised takeover, change, damage or destruction;
 - b) be deleted as soon as their usefulness ceases.

V

A person using a laptop computer containing personal data shall be obliged to take a special precautions while having the laptop computer transported, stored or used outside the area referred to in § 4 paragraph 1 of the Regulation, including cryptographic protection measures.

VI

Devices, discs and other electronic information media containing personal data intended to:

- 1) liquidation – are to be devoid of those data record in the first place, and in the case when it is impossible, the records are damaged, thereby to make them not readable.
- 2) be turned over to any other party unauthorised to process personal data – are to be devoid of the personal data records, thereby to make them not retrievable.
- 3) be repaired – are to be devoid of those data record, thereby to make them not retrievable or repaired under a supervision of a person who has been authorised by the controller.

VII

The controller shall supervise the security measures to be implemented within the computer system.

B. Security measures at the medium security level

VIII

In case where the password is used for user authentication, the password shall consist of at least 8 characters, including small and capital letters, numbers and special characters.

IX

Any devices and information media containing personal data referred to in Art. 27 paragraph 1 of the Act of August 29, 1997 on Personal Data Protection being transferred outside the area referred to in § 4 point 4 of the Regulation shall be secured in such a way to ensure confidentiality and integrity of these data.

X

The computer system management instruction referred to in § 5 of the Regulation shall additionally cover a method of the application of measures referred to in point IX of the Appendix.

XI

At the medium security level the controller shall apply security measures referred to in part A of the Appendix, unless the rules covered by part B provide otherwise.

C. Security measures at the high security level

XII

1. The computer system used for personal data processing shall be secured against any dangers originating from the public network by the implementation of a physical and logical security measures protecting from any unauthorised access.
2. In case where the logical security measures referred to in paragraph 1 are applied, these measures shall cover:
 - a) control of data flow between the computer system of the controller and the public network;
 - b) control of actions initiating from the public network and the computer system of the controller.

XIII

The controller shall apply a cryptographic protection measures for the data used for authentication which are being transferred within the public network.

XIV

At the high security level the controller shall apply the security measures referred to in part A and B of the Appendix, unless the rules covered by part C provide otherwise.