

The Regulation of June 3, 1998
By the Minister of Internal Affairs and Administration
As regards establishing basic, technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing.
(Journal of Laws of June 30, 1998, No. 80, item 521)

Pursuant to Art.45.1 of the Personal Data Protection Act of August 29, 1997 (Journal of Laws of 1997, No. 133, item 883 with later amendments) the following provisions have been adopted:

§1(1)

(deleted)

§2(2)

In order to have security of data appropriately managed within the computer system, the controller before starting to process personal data, is obliged to:

- 1) define aims, the strategy and the policy of data security within computer systems in which personal data are processed,
- 2) identify and analyse any danger and risk to which personal data processing may be exposed,
- 3) define needs as regards security of personal data files and computer systems including the cryptographic protection of personal data, in particular during their delivery by means of devices used for data transmission,
- 4) define security measures appropriate to any danger and risk,
- 5) screen functioning of security measures to be implemented in order to protect and thereupon process personal data,
- 6) work out and implement a training programme as regards the security of data within computer systems,
- 7) detect and react appropriately if any violation of security, either of personal data or of computer systems, has been revealed.

§3

The controller appoints a person, hereinafter referred to as "an administrator of information security", who is responsible for personal data security within the computer system, in particular for counteracting against making the data processing systems be available for unauthorised persons and for taking appropriate actions where a breach of the security system has been revealed.

§4

Individual job specifications of the persons employed to process personal data should define an area of this person's responsibility for the protection of the data against unauthorised access, groundless modification or deletion, illegal disclosure or collecting - to the extent adequate to this person's tasks in personal data processing.

§5

Before any person is allowed to work on personal data processing, he/she should be acquainted with regulations as regards personal data protection.

§6

1. The controller is obliged to work out an instruction of conduct in cases when personal data protection has been violated; the instruction is designed for employees working on personal data processing.
2. The instruction as mentioned in para.1 stipulates a mode of conduct in cases when:
 - 1) the violation of data security within computer system has been revealed,
 - 2) the state of the appliances, contents of the personal data file, revealed methods of work, procedures of programme functioning or the quality of communication within the telecommunication network indicate any breach of the data security.
3. In cases as referred to in para. 2 the person, who processes the data, is obliged to notify such an instance without delay to the administrator of information security or any other authorised person.

§7

1. The Controller determines which buildings, premises or their parts comprise the area where personal data are processed by means of stationary computer equipment.
2. A person who has not been authorised to gain access to personal data may stay inside the area, as referred to in para. 1, only in the presence of a person employed to process such data and with the direct consent of the controller or any other authorised person.
3. Buildings or premises where personal data are processed should be in the absence of persons working on data processing locked in such a way that would make impossible for any third parties to get inside.

§8

The power supplied devices and computer systems used for personal data processing should be protected against data loss which may be caused by any power supply failure or line interference.

§9

With the purpose of preventing an authorised person from any access to those data a person using a laptop computer for personal data processing is obliged to take precautions while having the laptop computer transported or stored outside the area, as referred to in §7 para.1, and he/she, in particular:

- 1) should secure access control and verification by means of a password,
- 2) should not give his/her permission to use a computer by a person unauthorised to any access to personal data.

§10

1. Devices, discs and other information media containing personal data are to be devoid of those data records in the first place if they are intended for liquidation, and in the case when it is impossible, the records are damaged, thereby to make them illegible.

2. Devices, discs and other information media containing personal data, are to be devoid of the personal data records in the first place if they are intended to be turned over to any other party unauthorised to receive personal data.
3. Devices, discs and other information media are to be devoid of the personal data records if they are intended to be repaired or they may be repaired under a supervision of a person who has been authorised by the controller.
4. Any printouts intended to liquidation, if they contain personal data should be damaged, thereby to make the data illegible.

§11

1. The controller is obliged to work out an instruction that would define the way in which the computer system used for personal data processing is to be managed. The instruction should, in particular, include requirements concerning information security.
2. The instruction, as referred in para.1, should comprise, in particular:
 - 1) a definition of how to lay down methods of passwords distribution between users and frequency of their changes and an indication of a person who is responsible for the aforesaid activities,
 - 2) a definition of how to lay down methods in which users will be logged in and out and an indication of a person responsible for the aforesaid activities,
 - 3) procedures of clocking employees in and out (measuring the beginning and the end of work),
 - 4) methods and frequency of making emergency copies,
 - 5) methods and frequency of computer virus detecting and deleting,
 - 6) methods and period of information media storing including data copies and printouts,
 - 7) methods of performing system and personal file service routine,
 - 8) procedures of communication within a computer network.

§12

1. Emergency copies, as referred to in §11.2.4 should not be stored in the same places as personal data files being currently processed.
2. The emergency copies should:
 - 1) be periodically checked from the point of view of their usefulness to data retrieval in a case of any system failure,
 - 2) be deleted as soon as their usefulness ceases.

§13

Information media and printouts including personal data which are not intended to any form of disclosure should be stored in such a way to protect them from any unauthorised access.

§14

1. The computer system in which personal data are processed should be equipped with user authentication mechanisms and access control and verification devices.

2. The administrator of information security is responsible for the proper control upon the functioning of the devices and mechanisms mentioned under alinea 1.
3. A separate identifier and a password should be established by the controller for each user of the computer system in which personal data are processed.
4. The identifier, as mentioned under alinea 1 is listed in the register, as referred to in Article 39.1 of the Personal Data Protection Act of August 29, 1997 (Journal of Laws of 1997, No. 133, item 883 with later amendments), hereinafter called the Act, including the user's name and his/her surname and it is registered in the computer system.
5. The direct access to personal data processed in the computer system is permissible only after the identifier and the proper password were accepted by the system.
6. The user's password should be changed at least once a month.
7. The user's identifier should not be changed, and in the case when the user has been registered out, the same identifier should not be allocated to another person.
8. The user's passwords giving access to computer system, shall be kept in secret also after their expiry date.
9. The identifier of a user that has lost its authorisation to personal data access, should be immediately registered out of the computer system in which these data are processed. Moreover, the password of such a person should be invalidated and other appropriate steps should be taken to prevent that person from unauthorised access to these data.

§15

1. If it is technically possible visual display units of computers where personal data can be accessed should be automatically shut out by means of screen savers after a specified period of non-operation.
2. In the premises where unauthorised persons may stay visual display units of computers in which personal data may be accessed shall be situated in a way so that these persons had no insight.

§16

For each person whose personal data are being processed in the computer system, that system should secure keeping records of:

- 1) a date when one's personal data have been registered for the first time,
- 2) data sources, if there is a possibility that they come from different sources,
- 3) an identifier of a user who registers the data,
- 4) information to whom, when and to what extent the data were disclosed, if such a disclosure to various bodies is permissible unless the data are generally available,
- 5) an objection, as referred to in Article 32.1.7 of the Personal Data Protection Act, after its acceptance, and another objection as referred in Article 32.1.8 of the same Act.

§17

The computer system used for personal data processing shall provide for disclosure of the content of each person's data in writing, in an intelligible form, including all the information as referred to in §16. if the data are processed.

§18

The controller of the data processed in a data file which has already existed on the day when the regulation becomes effective, is obliged to perform activities as mentioned in §2 at three month's notice since the day of its implementation.

§19

The regulation shall enter into force after 14 days since its promulgation.

Footnotes:

- 1) §1 in following wording: "Any time in this regulation the reference is made to :1) computer system - it means a system of data processing as well as its technical and financial resources, which supplies and distributes information, together with the people concerned, 2) security of the computer system - it means an implementation of appropriate administrative, technical, and physical measures applied to protect technical resources and personal data against any modification, deletion, unauthorised access, disclosure and collecting as well as accidental loss" is deleted by the amendment.
- 2) For the purpose of the Personal Data Protection Act of 29 August 1997 the expression "a data administrator" is used which stands for "a controller" - used in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.