Instructions for managing the IT system used for data processing

in AVSI POLSKA

Chapter 1

General

§ 1

Pursuant to the provisions of Article 24(2) of the Regulation (EU) of the European Parliament and of the Council of 27 April 2016 and the Act of 10 May 2018 on the protection of personal data, the content of the Instructions for managing the IT system used to process personal data in AVSI POLSKA, hereinafter referred to as the Instruction, is established.

§ 2

The Instruction applies in the area indicated in the Security Policy for the processing of personal data at AVSI POLSKA (hereinafter referred to as the Security Policy), in which personal data is processed in the IT system.

§ 3

The personal data administrator exercises general control and supervision over compliance with the provisions of the instructions, in particular:

1) himself or with the help of a person designated by him/her, makes backup copies for network databases;

2) deprives devices and other data carriers intended for the deletion of data recording on their own or – if this is not possible – permanently damages them in a way that makes it impossible to read the data;

3) supervises the removal of computer hardware failures in a way that ensures the security of the processed personal data;

4) he/she secures personal data files sent outside the area specified in the Security Policy on his/her own or with the help of a person designated by him/her;

5) supervises the physical security of the premises where personal data is processed;

6) he/she supervises activities related to virus protection, maintenance activities related to the IT system in which personal data is processed or with the help of a designated person;

7) supervises the circulation and processing of printouts from the IT system containing personal data;

8) undertakes and supervises all other activities aimed at ensuring the security of personal data processed in the IT system.

§ 4

Whenever the Instruction refers to:

1) **IT system** – it should be understood as a set of cooperating devices, programs, information processing procedures and software tools used for data processing;
2) **securing the IT system** – it should be understood as the applied technical and organizational measures ensuring the protection of the processed personal data appropriate to the threats and categories of data subject to protection, aimed in particular at protecting the data against their disclosure to persons unauthorized access, removal by unauthorized person alteration, loss, damage to the destruction;
3) **personal data set** – means any structured set of personal data, available according to specific criteria, regardless of whether this set is dispersed or functionally divided;

4) **data processing –** it means any operations performed on personal data, such as collecting, recording, storing, developing, changing, making available and deleting, and in particular those performed in IT systems;
5) **data deletion** – it means the destruction of personal data or such modification that will not allow to determine the identity of the data subject;
6) **user** – means an employee authorized by the data administrator (in the case of appointing an information security administrator also by the Information Security Agency), designated to process personal data;
7) **user identifier (login)** – it shall be understood as a sequence of letter, digit or other characters, unambiguously identifying the person authorized to process personal data in the IT system;
8) **password** – it means a sequence of letter, digital or other characters, assigned to the user identifier, known only to a person authorized to work in the IT system;
9) **authentication** – it is understood as an action aimed at verifying the declared identity of the entity;
10) **personal data carriers** – it means floppy disks, CDs or DVDs, flash drives, hard drives, magnetic tapes or other devices/materials used to store data files.

Chapter 2

Scope of the Instruction

§ 5

This Manual contains in particular:

1) the method of assigning passwords to users and the frequency of their change, as well as indicating people responsible for those activities;
2) the method of registering and deregistering users and indicating the persons responsible for these activities;
3) the procedures for starting, suspending and terminating work;

4) methods and frequency of emergency backups;
5) method and frequency of checking for the presence of computer viruses and the method of their removal;
6) the manner and duration of storage of information carriers, including computer copies and prints;
7) the method of inspection and maintenance of the system and the personal data set;
8) the procedure for communication in a computer network.

§ 6

The Instruction covers:

1) persons employed in the processing of personal data;
2) persons who have access to the processing of personal data

Chapter 3

GRANTING AUTHORIZATIONS TO PROCESS DATA AND REGISTERING THEM IN THE IT SYSTEM

§ 7

1. Only a person with the appropriate authorization and registered in the register of users can be a user of an IT system.

2. The register of users of the system shall be kept by the responsible person and shall be recorded and is updated in a secure folder.

3. Each registered user uses the user account assigned to him, which is provided with an access ID and password.

4. Assigning IDs and assigning passwords

1) It is recommended that the password should be at least 8 characters long; contained lowercase and uppercase letters and numbers and special characters;
2) user ID should be different for each user, and once it is deregistration from the IT system should not be assigned to another person;
3) user identifiers are disclosed in the list of persons authorised to provide processing of personal data;
4) passwords remain secret, each user is obliged to keep their password secret, even after it has been changed;
5) the password with which there is even a suspicion of disclosure should be immediately changed by the user;
6) Loss of authorization to process personal data results in immediate removal from the group of users of the IT system.

§ 8

1. The individual scope of activities of the authorised person in the processing of personal data should specify the scope of responsibility of this person for the protection of such data against:

1) unauthorised access;
2) unreasonable modification or destruction;
3) disclosure;
4) acquisition – to the extent appropriate to the tasks of this person in the processing of data

   Personal.

2. If possible, the screens on which personal data can be accessed should be automatically turned off after a set period of user inactivity.

3. Computer monitors should be set up in such a way as to prevent unauthorized persons from viewing personal data.

Chapter 4

Procedures for starting, suspending and terminating work in the IT system

§ 9

1. Before starting work in the IT system, the user is obliged to:

1) logging in to the system using the identifier and password reserved only for themselves in a way that prevents their disclosure to third parties – the password cannot contain less than 8 characters, the person creating it is obliged to do it in such a way as to make it difficult to read, if any, by entering into the password: special characters, numbers, capital letters, etc.,
2) checking the correct functioning of computer equipment and systems, on the basis of your workplace,
3) If any irregularities are found, to notify the immediate superior of this fact
4) In the event of a breach of the security of the IT system or a state indicating the existence of such a possibility, to take appropriate steps in accordance with the rules of conduct in the event of a breach of personal data security.

2. When interrupting data processing, the user should at least: activate the screen blank or otherwise block the use of his user account by other persons. It is recommended in such cases:

1) using the mechanism of temporary blocking of access to the computer by running a screen saver with a password (the password should coincide with the password for logging into the system);

2) termination of work in the IT system – logging out of the system.

3. After the completion of the processing of personal data on a given day, the authorized person is obliged to:

1) termination of work in the IT system;

2) logging out of the IT system;

3) turning off computer equipment and locking cabinets in which the media on which personal data are stored are stored;

4) closure of rooms.

4. Information carriers and printouts with personal data that are not intended to be made available are stored in conditions that prevent unauthorized access to them.

Chapter 5

Backups

§ 10

Devices and IT systems used for the processing of personal data, powered by electricity, should be protected against the loss of such data due to power failure or disturbances in the power supply. This protection should be constructed in such a way as to It allowed you to save data in all running applications and make a backup.

§ 11

1. Backups are made at different intervals depending on the system in question, but at least once a week.
2. Backups are created automatically by scheduled tasks in IT system
3. The person responsible for creating backups is an IT specialist.
4. Backup copies should be described in a way that allows for determining the their contents.
5. Backup copies that have been damaged or become unnecessary are deprived of data recording in a way that makes it impossible to restore them.
6. If de-recording is not possible, the copies shall be destroyed in such a way as to prevent the reading or restoring the data contained on the copy carrier.

Chapter 6

Method and duration of storage and rules for the disposal of information carriers

§ 12

1. Computer printouts from the system, containing personal data, are made only for operational objectives.
2. A computer printout from the system, containing personal data, after appropriate description and marking, is subject to the rules of protection of personal data processed by traditional methods.
3. Printouts from personal data files created and used for working purposes (operating) are stored in lockable cabinets.
4. Magnetic, optical and other IT media containing personal data are stored in appropriate, lockable cabinets.
5. Removal of printouts containing personal data from the system is carried out with the use of a document shredder or in another way that makes it permanently impossible to read the data.
6. Devices, disks or other IT media that have been intended to be transferred to another entity are deleted from the data stored on them.

Chapter 7

Antivirus protection

§ 13

1. Anti-virus protection is provided by installing appropriate anti-virus software.
2. In the event of detecting a computer virus, the system user is obliged to immediately inform the personal data controller about this fact
3. The IT system, including workstations and servers, is subject to constant monitoring and periodic full scans for the presence of computer viruses.

4. Detected threats are immediately removed from the IT system.

5. Before proceeding to neutralize the virus, it is necessary to protect the data contained in the system against their loss.

6. The person responsible for the above activities is an IT specialist

Chapter 8

Maintenance and repair of the system that processes personal data

§ 14

1. Current work in the field of maintenance and repair of the personal data processing system is carried out by the person responsible for these activities or, if it is necessary to involve an entrepreneur professionally involved in their performance, they are performed under the direct supervision of the personal data administrator or an IT specialist.

2. Computer devices, hard drives, or other computer data carriers intended for repair are deprived of the recording of personal data stored on them before these activities.

Chapter 9

Procedures for communication in a computer network

§ 15

1. Any files containing copies of personal information contained in the system that are sent outside the system must be password protected.
2. As far as possible, personal data contained on a web server may not be stored on workstations. This data should be placed on a network drive.
3. Unjustified copying of data from the server to workstations or media information technology is prohibited.

Chapter 10

Rules for using portable computers

§ 16

1. A person using a portable computer used for the processing of personal data is obliged to exercise special caution when transporting and storing this computer outside the area intended for the processing of personal data, indicated in the Security Policy.
2. In order to prevent unauthorized access to this data, you should:
   1) secure access to the computer with a password (in the case of Windows operating system) – in the manner that the software makes possible);
   2) Do not allow unauthorized persons to use the computer to access personal data;
   3) protect applications that process personal data with a password.

Chapter 11

Procedure in the event of a personal data breach

§ 17

A breach of the security of the IT system is in particular:

1) breach or attempt to breach the integrity of the system intended for the processing of personal data – by persons unauthorised to access the network or application with the personal data set;
2) breach or attempt to breach the integrity of personal data in the processing system (any modification, destruction, deletion of personal data by an unauthorized person made or attempted);
3) intentional or unintentional transfer of a set of personal data to a person who is not authorized to receive them;
4) unauthorized logging into the system;

5) unauthorized work on the account of the user authorized to process data personal data by an unauthorised person;
6) the existence of unauthorized accounts to access personal data;
7) hacking or attempted hacking from outside the network;
8) unauthorized changes to data in the system;
9) failure to block access to the system by the person authorized to process personal data during his or her absence;
10) disclosure of individual user access passwords to the system;
11) lack of supervision over service technicians or other employees staying in the rooms where personal data processing takes place;
12) unauthorized access or attempted access to the premises where the processing of personal data takes place;
13) theft of media on which personal data is stored;
14) unauthorized change or deletion of data saved in backup or archival copies;
15) failure to make a backup copy in a timely manner;
16) improper or unauthorized damage or destruction of media containing personal data.

§ 18

In the cases referred to in § 17, actions should be taken to secure the scene of the crime, secure any evidence of the crime and minimize the damage caused, including in particular:

1) record all information related to a given event, in particular:
   1) the exact time of obtaining information about the personal data breach and the time of self-detection of this fact,
   2) the data of the reporting person,
   3) description of the scene of the incident,
   4) a description showing the technical condition of the equipment used to process or store personal data, any established circumstances of the event;
2) generate and print all possible documents and reports on an ongoing basis, which can help;

3) identify the event by determining in particular:
   1) the extent of the damage,
   2) the manner in which the unauthorised person gained access to the personal data,
   3) the type of data affected by the breach;
4) eliminate the factors of imminent risk of personal data loss;
5) draw up a report of the above-mentioned activities;
6) inform the competent law enforcement authorities in the event of a suspicion of committing a crime.

§ 19

The personal data administrator or a person authorized by him is obliged to immediately take action to stop or limit unauthorized access to personal data, in particular by:

1) changing passwords for administrators and users
2) physical disconnection of devices and network segments that could allow access to the database by an unauthorized person;
3) logout of a user suspected of a data breach

§ 20

After analysing the causes and consequences of the event causing a breach of the security of the processed personal data, the persons responsible for the security of personal data are obliged to take all other actions aimed at eliminating similar breaches in the future and reducing the risk of their negative effects. In particular, if the cause of the infringement is:

1) error of the person authorized to process personal data related to the processing of personal data - additional individual or group training should be conducted;
2) activation of a computer virus - its source should be determined and an anti-virus protection test should be performed;
3) negligence on the part of the person authorized to process personal data - consequences must be drawn in accordance with the provisions of labor law on employee liability;

4) burglary - a detailed analysis of the implemented security measures should be performed;

5) poor condition of the device or the way the program works or other imperfections of the IT system for processing personal data - maintenance and programming inspections should be carried out immediately.poor condition of the device or the way the program works or other imperfections of the IT system for processing personal data – control service and software activities should be carried out immediately.

§ 21

In the event of damage to the data processing equipment, loss of data or their distortion, personal databases are restored from the last backup.

§ 22

1. The personal data administrator or a person authorized by him is obliged to prepare a report on the event violating the security of the IT system, including conclusions regarding the entire ICT process of personal data processing, in particular:
   1) the condition of the devices used to process personal data;
   2) the content of the personal data set;
   3) the correctness of the operation of the IT and ICT system in which personal data is processed, taking into account the effectiveness of the measures applied until the breach occurs against unauthorised access;
   4) the quality of IT network operation;
   5) exclude the presence of computer viruses;
   6) determine the cause and course of the event;
   7) conclusions on how to avoid similar infringements in the future.
2. The report referred to in paragraph 1 shall be submitted to the data controller within 30 days from the date of confirmation of the IT system security breach.

Chapter 12

Final provisions

§ 23

In matters not regulated by the provisions of the Act of 10 May 2018 on the protection of personal data (consolidated text: Journal of Laws of 2018, item 1000) and the provisions of the Regulation of the European Parliament and of the Council (EU) of 27 April 2016, shall apply.