Personal data security policy

Personal data processing security policy

in the AVSI POLSKA association with its registered office in Warsaw,

Chapter 1

General

§ 1

The purpose of the Security Policy for the processing of personal data at AVSI POLSKA, hereinafter referred to as the "Security Policy", is to obtain an optimal and compliant with the requirements of applicable legal acts method of processing information containing personal data.

§ 2

The security policy was created in connection with the requirements contained in the Regulation of the European Parliament and of the Council (EU) of 27 April 2016 and the Act of 10 May 2018 on the protection of personal data.

§ 3

Personal data protection is implemented through physical, organizational,
system software, applications, and users.

For the effective implementation of the Security Policy, the personal data administrator ensures:

a) Technical measures and organisational measures appropriate to the risks and categories of data to be protected;

b) Control and supervision over the Processing of personal data;

c) Monitoring of the protective measures used.

§ 4

1. Maintaining the security of the processed personal data in AVSI POLSKA is understood as ensuring their confidentiality, integrity, accountability and availability at an appropriate level. The measure of security is the size of the risk associated with the protection of personal data.
2. The security measures used are to achieve the above objectives and ensure:
   1) confidentiality of data – understood as a property ensuring that data is not made available to unauthorized persons;
   2) data integrity – understood as a property ensuring that personal data has not been altered or destroyed in an unauthorized manner;
   3) data accountability – understood as a property ensuring that a person's actions can be unambiguously attributed only to that person;
   4) integrity system integrity – understood as the inviolability of the system, impossibility any manipulation, whether intentional or accidental;
   5) availability of information – understood as ensuring that authorised persons have access to information and related resources when it is needed;
   6) risk management – understood as the process of identifying, controlling and minimizing or eliminating security risks that may relate to information systems used to process personal data.

§ 5

1. The administrator of personal data processed by AVSI POLSKA is the Management Board.

Chapter 2

Definitions

§ 6

The terms used in the Security Policy should be understood as:

1) Act – means the Act of 10 May 2018 on the Protection of Personal Data (consolidated text: Journal of Laws of 2018, item 1000);
2) Regulation – Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data;
3) personal data - any information relating to an identified or identifiable natural person;
4) personal data set – any structured set of personal data, available according to specific criteria, regardless of whether this set is dispersed or functionally divided;
5) 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;
6) IT system – means a set of cooperating devices, programs, information processing procedures and software tools used to process personal data;
7) traditional system – means a set of organizational procedures related to the mechanical processing of information and equipment, and fixed assets for the purpose of processing personal data on paper;
8) data protection in the IT system – it is understood as the implementation and operation of appropriate technical and organizational measures to ensure the protection of data against unauthorized processing;
9) IT system administrator – means a person or persons authorized by the personal data administrator to administer and manage IT systems;
10) user – means an employee authorised by the Personal Data Administrator or the Information Security Administrator (if appointed), appointed to process personal data;
11) user identifier (login) – a sequence of letter, digit or other characters, unambiguously identifying a person authorized to process personal data in the IT system;
12) password – a sequence of letters, digits or other characters, assigned to an identifier known only to a person authorized to work in the IT system.

Chapter 3

SCOPE

§ 7

1. In particular, AVSI POLSKA processes personal data of employees and customers (including contractors, employees, associates, members of governing bodies, customers) collected in personal data files.
2. This information is processed both in the form of traditional and electronic documentation.
3. The security policy contains documents concerning the technical and organizational safeguards introduced to ensure the protection of the processed personal data.
4. The personal data controller does not undertake processing activities that could be associated with a serious probability of a high risk to the rights and freedoms of individuals. If such an action is planned, the Personal Data Controller will perform the activities specified in Article 35 et seq. of the GDPR.
5. The Personal Data Controller keeps a register of processing activities, the template of which is attached as an Appendix to this Policy.

§ 8

The security policy applies in particular to:

1) personal data processed in the system: Comarch ERP XL, Comarch ERP Optima, Payer, Microsoft Office, Office 365;
2) all information concerning customer data (including contractors, employees, associates, members of bodies, customers) and employees;
3) all customer data (including contractors, employees, associates, members of bodies, customers) and employees;
4) information on the security of personal data, including in particular account names and passwords in personal data processing systems;
5) register of persons authorised to process personal data;
6) other documents containing personal data.

§ 9

1. The scopes of personal data protection specified in the Security Policy apply to IT systems in which personal data is processed, and in particular to:
   a) all existing, currently implemented or future IT and paper systems in which personal data subject to protection is processed;
   b) all locations - buildings and rooms where protected information is or will be processed;
   c) all employees, associates and other persons having access to the protected information.
2. All employees, associates and other persons having access to protected information are obliged to apply the principles set out in the Security Policy, strictly comply with the scope of the authorization granted, process data and protect personal data in accordance with the regulations, report incidents related to data security breaches and improper functioning of the system.
3. The Personal Data Controller ensures in particular that:
   a) employees or co-workers are adequately prepared to perform their duties;
   b) each of the Personal Data processors was authorized in writing to process in accordance with the Authorization to process personal data – the template of the Authorization is attached to this Policy.
   c) each employee/co-worker undertook to keep personal data processed by AVSI POLSKA confidential – the statement is part of the Authorization to process personal data.

Chapter 4

List of personal data files

§ 10

1 . Personal data are collected in the following files:

1) Personal files of employees
2) Employee payrolls;
3) Customer Payroll
4) Employees' insurance declarations and data sent to the Social Insurance Institution
5) Collaborator data
6) Authorization set
7) Contractors' data
8) Archival documents
9) Agreements concluded with clients/donors/beneficiaries
10) Company and statutory documents – AVSI POLSKA
11) Email
12) Newsletter
13) Collection of recruitment documents

§ 11

The personal data files listed in § 10 section 1 points 1, 3, 7-12 are subject to processing in a traditional way, except for the files specified in points 2, 3-6, 13, which are collected and processed using an IT system.

Chapter 5

List of buildings, rooms and areas for the processing of personal data

§ 12

1. Personal data is processed in the building located in AVSI POLSKA at 9/2 Flory Street in Warsaw 00-586.

2. Appendix No. 1

Chapter 6

LIST OF PERSONAL DATA FILES WITH AN INDICATION OF THE PROGRAMS USED TO PROCESS THIS DATA

§ 13

Appendix No. 2

Chapter 7

STRUCTURE OF DATA SETS INDICATING THE CONTENT OF INDIVIDUAL FIELDS INFORMATION

§ 14

Structure of data sets indicating the content of individual information fields for programs and systems used in AVSI POLSKA are presented as follows:

Appendix No. 3

Chapter 8

HOW DATA FLOWS BETWEEN SYSTEMS AND HOW THEY WORK TOGETHER INFORMATION SYSTEMS WITH DATA SETS

§ 15

Data flow between individual systems

Appendix No. 4

Chapter 9

Technical and organizational measures to safeguard personal data

§ 16

1. Organizational security
   1) a Security Policy has been drawn up and implemented;
   2) the Instruction for managing the IT system used to process personal data was prepared and implemented
   3) only persons with authorizations granted by the data administrator or a person authorized by him have been allowed to process data;
   4) a procedure has been created in the event of a personal data breach;
   5) persons employed in data processing have been familiarized with the regulations on the protection of personal data and in the field of IT system security;
   6) persons employed in the processing of personal data are obliged to keep them confidential;
   7) the processing of personal data is carried out in conditions that protect the data against access by unauthorized persons;
   8) the presence of unauthorized persons in the premises where personal data is processed is allowed only in the presence of a person authorized to process personal data and in conditions ensuring data security;
   9) Documents and data carriers containing personal data that are subject to destruction are neutralized with the use of devices designed for this purpose or by modifying them in such a way that their content cannot be reconstructed, so that after the data is deleted, it is impossible to identify the persons.
2. Technical security
   1) internal computer network was secured by separating it from the public network using a ROUTER with built-in firewall functionality
   2) computer workstations are equipped with individual antivirus protection,

3) the computers are protected against the possibility of unauthorized persons using them to process personal data by means of an individual user ID in desktop computers, and in the case of portable computers, additionally with a password protecting the hard drive by encrypting data.

4) using a shredder to effectively remove documents containing personal data.

3. Physical protective equipment:

1) the area where personal data is processed, outside working hours, is protected by a security company,

2) the area of personal data processing is monitored 24 hours a day,

3) devices used to process personal data are located in locked rooms.

Chapter 10

TASKS OF AN IT SPECIALIST

§ 18

1. An IT specialist is responsible for:

1) ongoing monitoring and ensuring the continuity of the IT system

2) optimization of IT system performance, installations and configurations network and server equipment

3) installation and configuration of system and network software

4) configuration and administration of system and network software and software protecting data protected against unauthorized access

5) supervision over the provision of emergency power supply for devices requiring it that affect the security of data processing

6) cooperation with suppliers of services and network and server equipment

7) management of emergency copies of system and network software configurations

8) managing emergency copies of personal data and resources enabling their processing

9) counteracting attempts to breach information security

10) granting, at the request of authorized persons, strictly defined access rights to information in a given system
11) management of licenses, procedures related to them
12) conducting anti-virus prophylaxis

2. The work of an IT specialist is supervised in terms of compliance with the Personal Data Protection Act, the Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on the documentation of personal data processing and the technical and organizational conditions that should be met by devices and IT systems used for the processing of personal data, and the Security Policy by the data administrator or the information security administrator.

Chapter 11

USER TRAINING

§ 20

1. Before being allowed to work with an IT system processing personal data or personal data files in paper form, each user should be trained in the protection of personal data in electronic and paper files.
2. The scope of the training should include familiarizing the user with the provisions of the Personal Data Protection Act and the executive acts and instructions issued on its basis and instructions applicable to the personal data administrator, as well as the obligation to comply with them.
3. The training ends with the student signing a statement of participation in the training and its understanding and commitment to comply with the principles of personal data protection presented during the training.
4. This document is stored in the personal files of users and is the basis for taking actions to grant them rights to use the IT system processing personal data.

Chapter 12

Entrusting the processing of personal data

1. The personal data controller may entrust the processing of personal data to another entity only by way of an agreement concluded in writing, in accordance with the requirements indicated for such agreements in Article 28 of the GDPR.

2. Before entrusting the processing of personal data, the Personal Data Controller obtains, as far as possible, information about the previous practices of the processor regarding the protection of personal data.

Chapter 13

FINAL PROVISIONS

§ 21

1. The personal data administrator is obliged to read the content of the Policy of each user.
2. All regulations concerning IT systems specified in the Policy also apply to the processing of personal data in databases maintained in any other form.
3. Users are obliged to apply the provisions of the Policy when processing personal data.
4. A person who, in the event of a breach of the security of an IT system or a reasonable suspicion of such a breach, has not taken the action specified in this document, and in particular has not notified the relevant person in accordance with the specified rules, as well as if he has not taken the appropriate action documenting this case, disciplinary proceedings may be initiated.

5. A disciplinary penalty imposed on a person failing to notify does not exclude the criminal liability of that person, in accordance with the Act, and the possibility of the employer bringing a civil suit against him or her for compensation for the losses incurred.

6. In matters not covered by the Policy, the provisions of the Act and the Regulation shall apply.