PERSONAL DATA SECURITY POLICY

in the Entity named:

Integris Systemy IT Sp. z o.o.

address:

ul. Lutycka 1, 60-415 Poznań

Table of contents

I INTRODUCTION

The Personal Data Security Policy, hereinafter referred to as the Policy, was prepared in connection with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter EU Regulation) and the Personal Data Protection Act.

This document is a set of consistent, precise rules and procedures according to which the Entity builds, manages and provides information and IT resources and systems. It establishes the actions to be performed and the manner of establishing the principles and rules of conduct necessary to ensure adequate protection of the personal data processed. The Policy establishes the principles of security of personal data processing, which should be observed and applied in the Entity by all persons processing personal data, along with reference to the appropriate legal grounds. The Policy regulates the principles of work organization on personal data sets processed in the IT system and traditional methods. It also describes the threats to the security of processed personal data and how to respond to security breaches.

This document also has an informative and educational function, by presenting the duties and responsibilities of persons related to the processing of personal data.

The entity applies measures appropriate to the situation to ensure information security.

This Policy is supplemented and supplemented by the Instruction on the Management of the IT System used for the processing of personal data (Appendix No. 1), establishing the method of managing the IT system used to process personal data.

II LEGAL BASIS

The principles of personal data processing in particular regulate:

- ✓ Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC
- ✓ Personal Data Protection Act of 29 August 1997
- ✓ Regulation of the President of the Republic of Poland of 3 November 2006 on granting the statute to the Office of the Inspector General for Personal Data Protection – issued on the basis of Article 13(3) of the Act,
- ✓ Regulation of the Minister of Internal Affairs and Administration of 22 April 2004 on the templates of personal authorization and service card of the inspector of the Office of the Inspector General for Personal Data Protection – issued on the basis of Article 22a of the Act,
- ✓ Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on the documentation of personal data processing and technical and organizational conditions to be met by devices and IT systems used to process personal data – issued on the basis of Article 39a of the Act,

- ✓ Regulation of the Minister of Internal Affairs and Administration of 11 December 2008 on the template for submitting a data set for registration to the Inspector General for Personal Data Protection – issued on the basis of Article 46a of the Act,
- ✓ Act on the provision of electronic services,
- ✓ Guidelines for the development and implementation of the security policy of the Inspector General for Personal Data Protection.

III GLOSSARY

ADO – Personal Data Administrator, which is a body, organizational unit, entity or natural person, deciding on the purposes and means of personal data processing.

ASI – IT System Administrator, who is a person designated by the Personal Data Administrator responsible for the proper functioning of hardware, software and their maintenance, to the extent indicated by ADO.

Personal data - any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to a physical, physiological, genetic, mental identifier, the economic, cultural or social identity of the natural person.

Sensitive data (special category of data) - data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, sexuality or sexual orientation and data on criminal convictions and violations of law or related security measures.

PUODO – President of the Office for Personal Data Protection, which is the authority appointed in the field of personal data protection**.**

Entity – the entity indicated on the first title page of the Policy, for the purposes of which this Policy is developed and implemented**.**

Policy – this document of the Personal Data Security Policy.

Data processing – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Information system – a set of cooperating devices, programs, information processing procedures and software tools used to process data.

Authorized – a person with a formal authorization issued by the Personal Data Administrator or by an appointed person authorized to process personal data.

Deletion of data – destruction of personal data or their modification, which makes it impossible to determine the identity of the data subject.

Data protection in the IT system – implementation and operation of appropriate technical and organizational measures to ensure data protection against unauthorized processing

Data set – a structured set of personal data available according to specific criteria, regardless of whether the set is centralized, decentralized, or dispersed functionally or geographically.

Consent of the data subject – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

IV PROCESSING OF PERSONAL DATA

Personal data

Personal data is any information relating to an identified or identifiable natural person. When deciding whether a particular piece of information or information constitutes personal data, the Entity makes an individual assessment, taking into account the specific circumstances and the type of means or methods needed in a specific situation to identify a person.

An identifiable person is 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 physical, physiological, mental, economic, cultural or social characteristics. Personal data will be both data that allows to determine the identity of a specific person, as well as those that do not allow immediate identification, but are, with a certain amount of cost, time and effort, sufficient to determine it.

Processing of personal data

The processing of personal data is permissible only if:

1. when the data subject has consented to the processing of his or her personal data for one or more specific purposes;
2. when processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
3. when processing is necessary for compliance with a legal obligation to which the controller is subject;

4. where processing is necessary to protect the vital interests of the data subject or of another natural person;
5. where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The subject does not process sensitive data (special category of data), except when:

1. the data subject has given explicit consent to the processing of those personal data for one or more specific purposes, unless Union or Member State law provides that the prohibition cannot be lifted by the data subject,
2. processing is necessary for the fulfilment of obligations and the exercise of specific rights by the controller or data subject in the fields of employment, social security and social protection law,
3. processing is necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent,
4. the processing is carried out in the course of a legitimate activity carried out with appropriate safeguards by a foundation, association or other non-profit-making body with political, philosophical or trade union purposes, provided that the processing concerns only members or former members of that body or persons in regular contact with it in connection with its purposes and that personal data are not disclosed outside that body without the consent of the persons, to whom the data relate,
5. the processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or in the exercise of justice by the courts;
7. processing is necessary for reasons of important public interest, on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject;
8. processing is necessary for the purposes of preventive health or occupational medicine, for the assessment of a worker's fitness for work, medical diagnosis, the provision of healthcare or social security, treatment or the management of health care or social security systems and services on the basis of Union or Member State law
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of Union or Member State law which provides for appropriate and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

Information obligations on data processing

In the case of collecting data from the data subject, the Personal Data Administrator provides him with all of the following information:

1. his identity and contact details and, where applicable, the identity and contact details of his representative;
2. where applicable, the contact details of the Data Protection Officer;
3. the purposes of the processing of personal data and the legal basis for the processing;
4. if the processing is based on Article 6(1)(f) of the EU Regulation – legitimate interests pursued by the controller or by a third party;
5. information on the recipients of the personal data or on the categories of recipients, if any;
6. where applicable, the intention to transfer personal data to a third country or an international organisation and whether or not the Commission has established an adequate level of protection;
7. the period for which the personal data will be stored or, where this is not possible, the criteria used to determine that period;
8. the period for which the personal data will be stored or, where this is not possible, the criteria used to determine that period;
9. the existence of the right to request from the controller access to, rectification, erasure or restriction of processing of personal data concerning the data subject, or the right to object to processing, as well as the right to data portability;
10. if the processing is based on consent – information about the right to withdraw consent at any time without affecting the lawfulness of the processing, which was made on the basis of consent before its withdrawal;
11. information on the right to lodge a complaint with a supervisory authority;
12. information whether the provision of personal data is a statutory or contractual requirement or a condition for the conclusion of a contract and whether the data subject is obliged to provide them and what are the possible consequences of failure to provide data;
13. the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the EU Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

The above principles do not apply if a provision of another law allows the processing of data without disclosing the actual purpose of their collection or if the data subject already has this information.

In the case of collecting data not from the data subject, the Personal Data Administrator is obliged to inform this person immediately after recording the data additionally:

1. the source of the personal data and, where applicable, whether they originate from publicly available sources;
2. the categories of personal data concerned.

The above rules do not apply if:

1. a provision of another law provides for or allows the collection of personal data without the knowledge of the data subject,
2. informing requires a disproportionate effort – in particular when data are processed for archiving, statistical and scientific research purposes,
3. it proves impossible to provide information,

4. the recording or disclosure of the data is expressly required by EU or national law,
5. this concerns professional secrecy under EU or national law.

Principles of data processing

The entity fulfils its obligations by exercising special care to protect the interests of data subjects, ensuring that these data are:

1. **processed in accordance with the law,**

   (Compliant with all legal norms, both those already existing at the time of entry into force of the EU Regulation and those that were only later introduced into the legal order. Legality refers to compliance with both substantive law and procedural rules).

2. **collected for specified, legitimate purposes and not subjected to further processing incompatible with these purposes,**

3. **factually correct and adequate in relation to the purposes for which they are processed,**

   (The information resulting from the data processed by the controller is true, complete and corresponds to the current state of affairs. The Personal Data Administrator processes data only to the extent that it is necessary to fulfill the purpose for which the data is processed by him).

4. **stored in a form that allows identification of the persons to whom they relate, no longer than it is necessary to achieve the purpose of processing.**

5. The Personal Data Administrator **applies technical and organizational measures to ensure the protection of processed personal data appropriate to the threats and categories** of data protected, and in particular should protect data against unauthorized access, removal by an unauthorized person, processing in violation of the Act and change, loss, damage or destruction.

In addition, the Entity ensures information security by:

1. **Confidentiality of information**
   (information is not made available or disclosed to unauthorized persons, unauthorized persons do not have access to data),
2. **Information integrity**
   (information is complete and not unaltered),
3. **Accountability of activities**
   (all relevant activities performed in the processing of data have been recorded and it is possible to identify the person who performed the given activity),
4. **operational reliability**
   (the actions performed lead to the intended effects).

Entrusting data processing

If it is necessary to process data by separate entities providing services to the Personal Data Administrator, he may entrust their processing. Entrustment of processing shall be based on a contract or other legal instrument governed by Union or Member State law and binding on the processor and the controller, specifying the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and the rights of the controller.

The Personal Data Administrator keeps the document of the Register of entities to which the Entity entrusts personal data (Appendix 4).

Entrustment does not consist in providing data. Sharing is transferring data to another entity (recipient of data), which becomes their administrator, and entrusting consists in processing data by an entity that is not the administrator of these data**.**

Data Sharing

Sharing personal data is one of the forms of their processing. Sharing personal data can be defined as any activity enabling entities other than the controller to become familiar with them.

1. It is irrelevant whether the provision of data is for a fee or not, for the act to be considered as sharing.
2. It is irrelevant whether the communication is made orally or in writing, by means of the public or by computer network, etc., for the act to be regarded as communication.
3. Sharing personal data with persons or entities authorized to receive them takes place under the law.
4. The personal data provided may only be used in accordance with the purpose for which it was provided.

The Personal Data Administrator or a person authorized by him keeps the document of the Register of entities to which the Entity provides personal data (Appendix 5). The document contains information on the provision of personal data to all entities, with the exception of:

1. persons authorized to process personal data,
2. data subjects,
3. state or local government bodies to which personal data are made available in connection with the proceedings.

Recording of processing activities

The Personal Data Administrator keeps a register of personal data processing activities for which he is responsible. It shall include all of the following information in that register:

1. the name and contact details of the controller and any joint controllers and, where applicable, of the controller's representative and the data protection officer;
2. the purposes of the processing;
3. description of the categories of data subjects and of the categories of personal data

4. the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
5. where applicable, transfers of personal data to a third country or international organisation, including the name of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the EU Regulation, documentation of appropriate safeguards;
6. where possible, the planned deadlines for erasure of each category of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The register of personal data processing activities constitutes Appendix 7 to this Policy.

V AUTHORIZATION TO PROCESS PERSONAL DATA

1. Only persons authorized to process personal data are authorized to process personal data
2. The purpose of this procedure is to minimize the risk of unauthorized access to personal data and loss of confidentiality by unauthorized persons.
3. The Personal Data Administrator is entitled to grant authorizations regarding the processing of personal data, by way of a written Authorization to process personal data (Appendix 3),
4. The Personal Data Administrator may appoint persons authorized to grant authorizations regarding the processing of personal data, by way of a written authorization.
5. The authorization to process personal data takes place only on the basis of an individual authorization granted in accordance with the provisions of the Act on the Protection of Personal Data.
6. Authorization to process personal data must take place before the data processing by an authorized person begins.
7. The Personal Data Administrator or a person authorized by him keeps the document of the Register of persons authorized to process personal data (Appendix No. 2).
8. If it is necessary to grant or change rights (e.g. due to employment of a person or change of job position), the Personal Data Administrator or a person authorized by him is obliged to check whether the person:

    a. has completed training in compliance with the rules of personal data security,
    b. will process personal data in the scope e and purpose specified in the Policy and instructions for managing the IT system.

9. Authorization to process personal data requires familiarization with the provisions on the protection of personal data, to the extent necessary for the activities performed under the granted authorization.
10. The Personal Data Administrator is responsible for organizing and conducting training or acquainting authorized persons in another form with the provisions on the protection of personal data.
11. The training in the field of personal data protection is confirmed by the person participating in it in the form of a written Confirmation of participation in the training (Appendix 6).

VI SUBJECTIVE OBLIGATIONS IN THE AREA OF PERSONAL DATA PROTECTION

Obligations of the Personal Data Controller

1. division of tasks and responsibilities related to the organization of personal data protection,
2. taking appropriate and necessary actions to ensure proper protection of personal data, in particular by drawing up and implementing appropriate organizational and technical conditions,
3. introduction to the use of procedures ensuring the correct processing of personal data,
4. in the event of a personal data breach, the controller shall notify PUODO without undue delay, no later than within 72 hours after the breach is discovered, unless it is unlikely that the breach would result in a risk to the rights and freedoms of natural persons,
5. if a given type of processing – in particular with the use of new technologies – due to its nature, scope, context and purposes is likely to result in a high risk to the rights and freedoms of natural persons, the administrator shall, before commencing processing, assess the effects of planned processing operations on the protection of personal data (in accordance with Annex 7 to this Policy).
6. enforcement of the development of security measures for the processing of personal data,
7. reviewing the effectiveness of the Personal Data Processing Security Policy,
8. ensuring compliance with the provisions on the protection of personal data, in particular by: organizing and supervising compliance with the principles of personal data protection both in IT systems as well as in personal data files kept in paper and electronic form,
9. keeping documentation describing the applied security policy for the processing of personal data (this Policy and the resulting instructions and procedures),
10. implementation of familiarization with the provisions on the protection of personal data and the risks associated with data processing by the Entity's employees,
11. ensuring control over what personal data, by whom and when they were entered into the file,
12. granting and waiving authorizations to process personal data in the Entity,
13. keeping a register of persons authorized to process data, containing the name and surname of the Authorized Person, the date of sending and termination, the scope of the Authorization to process personal data, identifier if the Authorized Person has been registered in the IT system used to process personal data,
14. ensuring that persons authorized to process personal data are acquainted with the provisions on the protection of personal data,
15. analysis of the situation, circumstances and causes that led to the breach of personal data protection and preparation of recommendations and recommendations regarding the elimination of the risk of their recurrence,
16. conducting actions in accordance with the Instruction in the event of unauthorized access to the database or breach of data security,
17. providing legal grounds for the processing of personal data from the moment of collecting personal data until their deletion,
18. care for the correct processing of personal data, in particular by ensuring the timeliness, adequacy and substantive correctness of personal data processed for the purpose specified by them,

Obligations of the IT system administrator

The scope of duties of the IT System Administrator is:

1. ensuring optimal continuity of the IT system,
2. supervising the work of external companies carrying out work on repairs and maintenance of IT systems containing personal data,
3. granting, changing and blocking rights to a given User to IT systems,
4. proper configuration of the IT system ensuring its security and limiting access to personal data by unauthorized persons,
5. monitoring the functioning of security measures implemented to protect personal data,
6. supervising the efficient operation of the backup system.
7. taking action in the event of detecting security breaches in the security system or suspected violations, e.g. the appearance of a virus in the system,
8. installation and configuration of software on individual workstations,
9. providing technical support (software and devices) for the Company's employees,
10. periodic verification of the installed software on individual users' workstations,
11. Laptop security
12. other activities provided for in the Security Policy, in particular Appendix No. 1 (IT System Management Manual).

Obligations of authorised persons

1. knowledge of the Policy and generally applicable law in the area of personal data protection processed by the Entity,
2. knowing, understanding and applying as far as possible all available measures to protect personal data and preventing unauthorized access to your workstation,
3. processing of personal data in accordance with applicable law and adopted regulations, within the limits of the authorization granted,
4. acting in accordance with established internal regulations regarding the processing of personal data,
5. keeping personal data and information on how to secure them confidential, also after termination of employment,
6. protection of personal data and measures processing personal data against unauthorized access, disclosure, modification, destruction or distortion,
7. informing about any suspected breaches or noticed breaches and weaknesses of the system processing personal data to the supervisor, who is obliged to inform the Information Security Administrator.

VII RISK ASSESSMENT AND REVIEWS

Taking into account the categories of processed data and the threats identified as a result of the risk analysis, a high level of security is applied.

1. A review of the state of protection processed by the Data Subject is carried out at least once a year.
2. The review of the state of protection of personal data processed by the Subject is carried out by the Personal Data Administrator or appointed internal controllers.
3. The review covers all areas of the Entity's activity and infrastructure elements in which compliance with the principles of personal data processing is required, in particular IT systems, physical and organizational security.
4. The controller prepares a review plan taking into account its scope and the necessary resources, such as time and number of persons carrying out activities.
5. The review is logged.
6. The controller prepares the results of the review, which it then forwards in the form of a Review Report to the Personal Data Administrator, or possibly also to the head of the inspected entity.
7. On the basis of the inspection report, the Personal Data Administrator initiates preventive or controlling actions.

VIII PERSONAL DATA SECURITY THREATS AND INCIDENTS

The security of the personal data processing process consists of accountability, confidentiality and integrity of the processed data. Accountability means the ability to attribute a person's actions unambiguously and exclusively to that person. Confidentiality is expressed by ensuring that the processed personal data is not made available to unauthorized entities. Integrity means ensuring that personal data cannot be altered or destroyed unauthorized.

In the event of a breach of personal data protection or a threat to them, each employee is obliged to inform the Personal Data Administrator, the appropriate person authorized by him or his supervisor about this fact. The authorized person or the employee's superior is obliged to notify the Personal Data Administrator.

Instructions on how to deal with a threat to the security of personal data

A threat to information security is a situation in which there is a threat of an incident. Example of a catalog of threats:

1. failure to comply with the Policy by data processors, e.g. not locking rooms, cabinets, desks, failure to apply password protection rules,
2. improper physical protection of documents, equipment or premises,
3. inadequate protection of IT software or hardware against leakage, theft or loss of personal data.

Conduct of the Personal Data Administrator or a person authorized by him in the event of a threat:

1. determining the scope and causes of the threat and its possible effects,
2. as far as possible, restoring the state in accordance with the principles of personal data protection,
3. initiating disciplinary action if necessary,
4. recommending preventive actions to eliminate similar threats in the future,
5. documenting the proceedings in the Register of Security Violations (Appendix 8).

Instructions for dealing with personal data security incidents

An incident is an information security breach due to availability, integrity and confidentiality. Incidents should be detected, recorded and monitored to prevent their recurrence. Example incident directory:

1. random internal event, e.g. computer, server, hard disk failure, user error, IT, data loss,
2. random external event, e.g. natural disasters, flooding, power failure, fire,
3. intentional incident, e.g. information leakage, disclosure of data to unauthorized persons, deliberate destruction of data, operation of computer viruses, hacking into premises or IT system (internal and external).

Conduct of the Personal Data Administrator or the appropriate person authorized by him in the event of an incident:

1. determining the time of the incident being an incident,
2. determining the scope of the incident,
3. identification of causes, effects and estimated damage,
4. preservation of evidence,
5. identification of persons responsible for the infringement,
6. removal of the consequences of the incident,
7. limitation of damage caused by the incident,
8. initiating disciplinary action,
9. recommending preventive actions to eliminate similar threats in the future,
10. documenting the proceedings in the Register of Security Violations (Appendix No. 8).

Authorized Person's conduct in the event of a threat until the arrival of the Personal Data Administrator or a person authorized by him:

1. refraining from starting or continuing work, as well as from taking any action that may result in the obliteration of traces of the infringement or other evidence,
2. securing elements of the IT system or files, primarily by preventing unauthorized access to them,
3. take, as appropriate, all necessary measures to prevent further risks that may result in the loss of personal data.

IX LISTS

List of buildings, rooms or parts of rooms forming the area in which personal data are processed.

The list of buildings is an internal document of Integris.

List of personal data files with an indication of the programs used to process this data.

The list of datasets is an internal Integris document.

Description of the structure of the datasets, indicating the content of each information field and the relationships between them

The description of the data structure is an internal Integris document.

Technical and organisational measures necessary to ensure the confidentiality, integrity and accountability of the data processed

Organizational measures

1. A security policy has been developed and implemented;
2. An IT system management manual has been developed and implemented;
3. an IT system administrator was appointed;
4. Only persons with valid authorizations granted by the data controller have been allowed to process data;
5. Records of persons authorized to process data are kept;
6. Persons employed in data processing have been made aware of the provisions on the protection of personal data;
7. Persons employed in the processing of personal data in the field of IT system security were trained;
8. Persons employed in the processing of personal data are obliged to keep them secret;
9. Computer monitors on which personal data are processed are set in a way that prevents third parties from viewing the processed data;
10. Backup copies of the personal data file are stored in a different room than the one in which the server on which personal data are processed on an ongoing basis is located;
11. The processing of personal data is carried out in conditions that protect the data against unauthorized access;
12. The presence of unauthorized persons in the rooms where personal data are processed is allowed only in the presence of a person employed in the processing of personal data and in conditions ensuring data security;
13. Written data processing agreements are used for cooperation with subcontractors processing personal data;
14. The Entity has a clean desk and screen policy.

Physical data protection measures

1. The personal data set is stored in a room secured with ordinary doors (non-reinforced, non-fire-proof).
2. The rooms in which the personal data set is processed are equipped with a burglar alarm system.
3. Access to the rooms in which personal data files are processed is covered by the access control system.
4. Access to the rooms in which the personal data file is processed is supervised by the security service during the absence of employees employed there.
5. Personal data files in paper form are stored in locked cabinets.
6. Backups/archives of the personal data set are stored in a closed non-metallic cabinet.
7. The room in which personal data files are processed is protected against the effects of fire by means of a free-standing fire extinguisher.

8. Documents containing personal data are destroyed mechanically using document shredders after expiration.

Hardware measures for information and telecommunications infrastructure

1. The set of personal data is processed using portable computers.
2. The computer used to process personal data is connected to the local computer network.
3. UPS devices were used to protect the IT system used to process personal data against the effects of power failure.
4. Access to the personal data set, which is processed on a separate computer station / laptop computer, has been protected against unauthorized launch using a password.
5. Access to the operating system of the computer in which personal data is processed is secured by means of an authentication process using a user ID and password.
6. Measures have been taken to prevent unauthorised copies of personal data processed using IT systems.
7. System mechanisms were used to force periodic change of passwords.
8. A system of registration of access to the personal data system/set was used.
9. Cryptographic data protection measures have been applied for personal data transmitted by teletransmission.
10. Access to teletransmission means has been secured through authentication mechanisms.
11. A disk array was used to protect personal data from the effects of disk memory failure.
12. Measures were taken to protect against malware such as worms, viruses, Trojan horses, rootkits.
13. A firewall system was used to protect access to a computer network.

Protection measures in software tools and databases

1. Means were used to register changes made to individual elements of the personal data file.
2. Measures have been taken to determine the access rights to the indicated scope of data within the framework of the processed personal data set.
3. Access to the personal data file requires authentication using a user ID and password.
4. System measures were taken to determine appropriate access rights to IT resources, including personal data files for individual users of the IT system.
5. A mechanism was used to force periodic change of passwords to access the personal data set.
6. Screensavers have been installed at workstations where personal data are processed.
7. A mechanism of automatic blocking of access to the IT system used to process personal data in the event of prolonged inactivity of the user's work was applied.

X FINAL PROVISIONS

1. The security policy is a document binding the Entity in the implementation, compliance and verification of the principles of personal data protection.
2. The security policy is a document applicable to all persons allowed to process personal data as part of the Entity's activities.
3. Any person authorized to process personal data as part of the Entity's activity is obliged to read this Security Policy.
4. Violation of the rules resulting from the Security Policy may constitute the basis for initiating disciplinary proceedings against the violator.
5. The initiation or conduct of disciplinary proceedings against a person violating the rules resulting from the Security Policy does not exclude the possibility of initiating criminal proceedings and pursuing claims from a civil action.
6. The security policy together with attachments enters into force on the day of its signing by the Personal Data Administrator.
7. With regard to matters not covered by the Security Policy, the provisions of the Personal Data Protection Act shall apply.
8. Appendix to this Policy are part of it subject to supplementation. List of attachments:
   - 8.1. Instructions for managing the IT system used to process personal data (Appendix 1),
     - A. Administrator password log,
     - B. Records of media containing personal data,
     - C. Records of repairs, inspections and maintenance of the IT system,
     - D. Records of activities in the IT system,
     - E. Appointment of an IT system administrator,
   - 8.2. Register of persons authorized to process personal data (Appendix 2),
   - 8.3. Authorization to process personal data (Appendix 3),
   - 8.4. Register of entities to which the Entity entrusts personal data (Appendix 4),
   - 8.5. Register of entities to which the Entity provides personal data (Appendix No. 5)
   - 8.6. Confirmation of participation in the training (Appendix 6),
   - 8.7. Model data protection impact assessment (Appendix 7),
   - 8.8. Register of security breaches (Appendix 8),
   - 8.9. Model contract for entrusting personal data (Appendix 9)
   - 8.10. Register of personal data processing activities (Appendix 10)