Personal data security policy

Regulation on the protection of personal data

GREEN TEAM GROUP

TRUE NATURE – PURE TRADITION

Table of Contents

I. INTRODUCTION

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

This document is a set of consistent, precise rules and procedures according to which the Entity builds, manages and provides resources, and information and IT systems. It establishes the actions to be taken and the methods of establishing rules of conduct necessary to ensure proper protection of personal data being processed. The security policy establishes the rules for the processing of personal data that should be followed and used in the Entity by all persons who process personal data. The security policy regulates the principles of work organization at the collection of personal data processed by the IT systems and by traditional methods. It also describes the security risks of personal data being processed 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 adequate methods to ensure the security of the personal data being processed.

In the case when there is absence of the appointment of the Data Protection Officer or the IT System Administrator, their duties to the extent permitted by law shall be entrusted to the Personal Data Administrator.

LEGAL BASIS

The rules for the processing of personal data are governed by the provisions of the generally applicable law, in particular:

- Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individual persons with regard to the processing of personal data and on the free flow of such data and the repeal of Directive 95/46/EC
- the Act on the protection of personal data of 29 August 1997.

GLOSSARY

APD – administrator of personal data, being an authority, organizational unit, entity or natural person, deciding about the purposes and means of processing personal data.

AITS – administrator of the IT System, being a person designated by the APD who is responsible for the proper functioning of the equipment, software and their maintenance, to the extent indicated by the APD.

Personal data – all information regarding an identified or identifiable individual; an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as first name and surname, personal identification number, location data, internet identifier or one or more specific factors determining physical, physiological, genetic, psychological, economic, cultural or social identity of an actual person.

Sensitive data (specific category of data) – data revealing racial or ethnic origin, political views, religious or ideological beliefs, trade union membership, genetic data, biometric data processed to uniquely identify a actual person, data on health, sexuality or sexual orientation, and data on convictions and violations of the law or related security measures.

Password — a sequence of literal, digital or other characters, known only to the person authorized to work in the IT system.

User identifier — a sequence of letters, digits or other characters uniquely identifying a person authorized to process personal data in the IT system.

Data integrity — a property that ensures that personal information is not altered or destroyed in an unauthorized way.

DPS – Data Protection Supervisor, being the person designated by the Administrator of Personal Data to supervise the use of technical and organizational measures ensuring protection of personal data being processed, relevant to the threats and categories of data covered by the data protection.

Authorized person – a person holding a formal authorization issued by the DPS or by a designated person, that is authorized to process personal data.

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

Security policy – it is this document of the Personal Data Security Policy.

Data confidentiality — a feature that ensures that personal information is not shared with unauthorized persons or entities.

Data processing – it means an operation or set of operations performed on personal data or personal data sets in an automated or non-automated manner, such as collecting, recording, organizing, arranging, storing, adapting or modifying, downloading, browsing, using, disclosing by sending, distributing or other types of sharing, matching or combining, limiting, deleting or destroying.

POPDP – President of the Office for Personal Data Protection, which is a body appointed for personal data protection matters.

Accountability — a feature that ensures that the actions of a person on personal data can be attributed in an unequivocal manner only to the person, and also a feature that provides the opportunity to prove the rights of persons whose personal data is processed.

IT system – a set of cooperating devices, programs, information processing procedures and software tools used for data processing.

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

Authentication — this is an action aimed at verifying the declared identity of a person or entity.

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

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

Consent of the data subject – means voluntary, specific, conscious and unambiguous representation of the will, whose the data concern, in the form of a declaration or an action of clear confirmation, that allows for the processing of personal data concerning him/her.

II. GENERAL INSTRUCTIONS FOR APD / DPS and AITS

This manual is intended for APD and DPS, and AITS if appointed.

DUTIES OF THE APD

1. providing a legal basis for the processing of personal data from the collection of personal data to its removal, in particular through the application of information obligations, consistent with the disclosure requirements template (**Annex no. 1**),
2. ensuring accountability, i.e. control over what personal data, by whom and when they were introduced, edited or deleted,
3. taking care of the proper processing of personal data, in particular by ensuring the topicality, adequacy and substantive correctness of personal data processed in the specified purpose,
4. taking care of the correct implementation of the principle of temporality, in particular by ensuring the deletion of personal data after the processing period,
5. implementation of procedures and security measures ensuring proper processing of personal data,
6. risk assessment of procedures – implemented and introduced, security measures, resources and processes of personal data processing using the risk analysis template (**Annex no. 2**),
   enforcing the development of security measures for the processing of personal data,
7. keeping documentation that describes the applied security policy of personal data processing (this Security Policy and the instructions and procedures resulting from it),
8. optional in the absence of the appointment of the DPS – keeping a register of personal data processing activities (**Annex no. 3**) and a register of categories of personal data processing activities processed on behalf of another administrator (**Annex no. 4**),
9. granting and revoking the authorizations for personal data processing in Entity by employees (**Annex no. 5**) and authorizations to process personal data in Entity by persons employed under civil law contracts (**Annex no. 6**),
10. keeping a register of employees authorized to process data (**Annex no. 7**) and a register of persons employed under a civil law contract authorized to process personal data (**Annex no. 8**),
11. implementing the means of acquainting with the provisions on the protection of personal data and rules on this subject and the risks associated with the processing of data by the employees of the Entity,
12. ensuring the familiarization of persons authorized to process personal data with the principles of personal data processing,
13. optional (not applicable if the DPS is not called-up) – appointment of the Data Protection Supervisor,
14. optional (not applicable if the DPS is not called-up) – providing funds and organizational separation for the Data Protection Supervisor, necessary for the independent performance of his/her tasks,
15. optional (not applicable if the DPS is not called-up) – documenting the appointment of the Data Protection Supervisor by completing the declaration on appointing the Data Protection Supervisor (**Annex no. 9**),
16. optional (not applicable if the DPS is not called-up) – notification to the President of the Office of Personal Data Protection upon the appointment of the Data Protection Supervisor,
17. optional – where this type of processing, in particular when using new technologies, by its nature, scope, context and objectives is likely to cause a high risk of violation of the rights or freedoms of natural persons, the administrator carries out an impact assessment prior to commencing processing planned processing operations for the protection of personal data (**Annex no. 10**),
18. conducting actions in accordance with the Instruction in case of unauthorized access to the database or data security breach,
19. in the case of a breach of personal data protection, the APD without undue delay, not later than within 72 hours after finding the violation – submits them to POPDP (**Annex no. 11**), unless it is unlikely that the violation would result in the risk of violation of the rights or the freedom of individuals,

20. analysis of the situation, circumstances and reasons that led to the violation of personal data protection and the preparation of recommendations and prescription regarding the elimination of the risk of their reoccurrence,
21. measuring, testing and evaluating the effectiveness of the implemented Security Policy and security measures.

DUTIES OF THE PERSONAL DATA SUPERVISOR:

If the DPS is not appointed, these obligations shall apply accordingly to the APD.

1. informing APD and its employees who process personal data about the duties incumbent upon them under the EU Regulation and other EU or Member State laws on data protection and advise them in this matter,
2. monitoring compliance with the Regulation, other Union or Member States' legislation on data protection and APD policies or with the processing in the field of personal data protection, including segregation of duties, activities raising awareness, training of personnel involved in processing operations and related audits,
3. keeping a register of personal data processing activities (**Annex no. 3**) and a register of categories of personal data processing activities processed on behalf of another administrator (**Annex no. 4**),
4. providing on-demand recommendations as to the impact assessment for data protection and monitoring its implementation,
5. cooperation with the supervisory body,
6. acting as a contact point for the supervisory body in matters related to processing, including prior consultations referred to in art. 36 of the EU Regulation, and, where appropriate, conducting consultations on all other matters,
7. if there is a premise, acting as a contact point for data subjects in all matters related to the processing of their personal data and exercising their rights under the relevant EU Regulation.

REGISTRATION OF THE PROCESSING OF PERSONAL DATA

The DPS, and in the absence of him/her, the APD keeps a register of personal data processing activities (**Annex no. 3**), for which he/she is responsible. This register shall contain all of the following information:

1. full name and contact details of the administrator and any co-controllers, as well as, where applicable, a representative of the administrator and the data protection supervisor;
2. purposes of processing;
3. description of the categories of data subjects and 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 to international organizations;
5. where applicable, the transfer of personal data to a third country or international organization, including the name of that third country or international organization, and in the case of transfers referred to in Article 49, paragraph 1, section 2 of the EU Regulation, documentation of relevant safeguards;
6. if possible, scheduled dates for deletion of individual categories of data;
7. if possible, a general description of the technical and organizational security measures referred to in Article 32, paragraph 1.

The exclusion of the obligation of keeping the register of processing activities applies in the cases specified in Art. 30, item 5 of the Regulation.

RISK ANALYSIS

The DPS, and in the absence of him/her, the APD, carries out a risk assessments.

Particularly:

1. processing of personal data,
2. significant resources of the Entity (such as server, server room, archive),
3. implemented security measures,

should be analyzed in the context of the risk of violating the rights or freedom of the data subject.

The risk assessment should be carried out with taking into account:

1. the nature of the processing of personal data,
2. the scope of personal data processing,
3. the context of the processing of personal data,
4. purposes of processing personal data,
5. the risk of violating the rights or freedom of natural persons with various probabilities and the importance of the threat.

The risk assessment can be performed by using *the risk assessment template (**Annex no. 2**)*.

On the basis of such a risk assessment, appropriate technical and organizational measures are implemented to ensure the processing of personal data in accordance with the provisions of generally applicable law, as well as to demonstrate such circumstances.

Chosen security measures shall, if necessary, be reviewed and updated.

When assessing whether the security level of the measures implemented is appropriate, consideration shall be given in particular to the risks associated with the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

SECURITY MEASURES

Taking into account the nature, scope, context and purposes of processing and the risk of violating the rights or freedom of natural persons with different probabilities and seriousness of risk, the APD implements appropriate technical and organizational measures to process in accordance with the EU Regulation and in order to be able to prove it. These measures shall be reviewed and updated where necessary.

Taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing and the risk of violating the rights or freedom of individual persons with different probability of occurrence and threat weight, the APD and the processing entity implements the appropriate technical and organizational measures to ensure a degree of security corresponding to this risk, including, but not limited to, if applicable:

- pseudonymisation and encryption of personal data,

- the ability to continually ensure the confidentiality, integrity, availability and resilience of systems and processing services,
- the ability to quickly restore the accessibility and access to personal data in the event of a physical or technical incident,
- regular testing, measuring and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

In the description of organizational security measures listed in the register of personal data processing activities, all organizational measures adopted to ensure the security of the personal data processing system are listed.

In the area of technical security measures listed in the register of personal data processing activities, all technical measures implemented to ensure the security of the personal data processing system are to be listed.

AUTHORIZATION FOR PROCESSING OF PERSONAL DATA

1. Only the authorized persons for processing of personal data in the Entity are entitled 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 to unauthorized persons.
3. The APD is entitled to grant authorizations (instructions) regarding the processing of personal data, by means of a written authorization to process personal data (**Annex no. 5** for employees and **Annex no. 6** for persons employed under civil law contracts),
4. The APD may nominate persons permitted to grant authorizations for the processing of personal data, by means of a written authorization.
5. The authorization to process personal data takes place only on the basis of individual authorization.
6. The authorization to process personal data must take place before the processing of data by the authorized person.
7. The APD or a person authorized by him/her shall keep a document of the register of persons authorized to process personal data on the basis of an employment contract (**Annex no. 7**) and on the basis of civil law agreements (**Annex no. 8**).
8. In case of necessity to grant or change entitlements (eg. due to employment or change of position), the APD or a person authorized by the APD is obliged to check whether the person:
   a. had received training in compliance with personal data safety rules,
   b. will process personal data to the extent and purpose specified in the Policy and IT system management instructions.
9. The authorization to process personal data requires familiarizing oneself with Security Policy and regulations regarding the protection of personal data to the extent necessary for the activities performed under the authorization.
10. The APD is responsible for organizing and conducting training on the principles of personal data processing or familiarizing persons authorized with the principles of personal data protection in a different form.

PROCEDURE TO BE FOLLOWED IN CASE OF BREACH OF DATA PROTECTION RULES FOR APD/DPS

A breach of personal data protection is a security breach leading to an accidental or unlawful:

- destruction,
- loss of,

- modification,
- unauthorized disclosure or
- unauthorized access to personal data,

sent, stored or otherwise processed. In case of a breach of personal data protection, the infringement procedure described below should be started.

In case of a breach of the rules on the protection of personal data, the DPS and in the absence of his/her appointment, the APD is obliged immediately:

1. inform the reporting person about the further course of the proceedings and recommend him/her appropriate actions,
2. if possible, restore to the state consistent with the principles of personal data protection,
3. determine the duration and nature of the breach, if possible defining the categories and approximate number of data subjects, as well as the categories and approximate number of entries of personal data affected by the breach,
4. determine the possible consequences of a breach of personal data protection,
5. recommend preventative measures to eliminate similar threats in the future,
6. in case of occurrence of premises specified in the EU Regulation, report the breach within 72 hours to the POPDP, taking into account the information included in the violation notification template to the POPDP (**Annex no. 11**),
7. if necessary, initiate disciplinary means,
8. document the proceedings in the register of personal data safety breaches (**Annex no. 12**).

III. GENERAL INSTRUCTIONS FOR THE I.T. SYSTEM ADMINISTRATOR

This manual is intended for the APD, and for the AITS if appointed. In the absence of an AITS appointment, these instructions and procedures apply to the APD.

DUTIES OF THE I.T. SYSTEM ADMINISTRATOR

1. implementation and maintenance of means of encryption of personal data processed within the Entity's IT system, in particular by means of cryptographic security protection of mobile devices used for processing personal data (e.g. laptops, smartphones),
2. proper configuration of the IT system used to process personal data in the Entity, in order to ensure its ability to continually ensure confidentiality, integrity, availability and resilience of processing systems and services,
3. care for maintaining and securing servers of the IT system used to process personal data in the Entity, regardless of whether the server is in the premises of the Entity or outside of it, and in particular ensuring its confidentiality, integrity, accessibility and resilience,
4. ensuring the ability of the IT system used to process personal data in the Entity, to quickly restore the accessibility and access to personal data in the event of a physical or technical incident,
5. regular testing, measuring and assessing the effectiveness of technical means of the IT system used to process personal data in the Agency, aimed at ensuring the security of personal data processing with its use,
6. installation, configuration, deletion, licensing and renewal of licenses, in relation to software used in ICT devices used in the Entity's IT system,
7. supervision over the work of external entities, carrying out work on repairs, maintenance of IT systems used to process personal data in the Entity, in order to ensure compliance of these activities with the rules adopted in the Entity,

8. assigning, changing and withdrawing identifiers and passwords as well as authorizations to use the applications and programs for persons authorized to process personal data in the Entity,
9. supervision over the correct implementation and functioning of the system for making backup copies of all information carriers, used for the processing of personal data in the Entity, in accordance with the adopted backup policy in the Entity,
10. taking action in case of suspected or detected security breaches in the security system of the IT system used to process personal data in the Entity,
11. providing technical assistance in the use of software and devices used within the IT system used to process personal data in the Entity,
12. securing of portable computers used to process personal data in the Entity,
13. securing the AITS passwords and providing access to them in situations of higher necessity (force majeure) inability of the AITS to use passwords, other activities provided for in the Security Policy.

PROCEDURE FOR INVENTORY

The AITS is required to record all activities performed in the IT system used to process personal data in the Entity, as well as to record devices and media used to process personal data. The registration takes place in:

1. Register of repairs, inspections and maintenance of the IT system (**Annex no. 13**),
2. The register of activities in the IT system (**Annex no. 14**),
3. The register of devices and media used to process personal data (**Annex no. 15**).

PROCEDURE FOR PERFORMING AUDITS OF SYSTEM ACCESS

The following requirements regarding system access audits to the IT system used to process personal data in the entity are established. The AITS is obliged to monitor and ensure compliance with them.

1. In the IT system used to process personal data in the Entity, mechanisms for audit access to such data are used.
2. If the access to personal data processed in the IT system (in particular to the devices, applications or programs, has at least two people, then it is ensured that:
    a. in this system a separate identifier was registered for each user,
    b. access to the data was possible only after entering the ID and authentication.
3. The IT system used to process personal data shall be secured, in particular against:
    a. operation of software aimed at obtaining unauthorized access from the IT system,
    b. loss of data due to power failure or interference in the power supply network.
4. The identifier of a user who has lost the right to process personal data can not be assigned to another person.
5. In the case when a password is used to authenticate users in the IT system used to process personal data, measures are employed to enforce the use of passwords consisting of at least 8 characters, including uppercase and lowercase letters as well as numbers or special characters.

ANTI-VIRUS PROTECTION PROCEDURE

The purpose of the procedure is to secure information systems against malicious software (e.g. worms, viruses, Trojans, rootkits) and unauthorized access to personal data processing systems. The following requirements regarding anti-virus protection are established. The AITS is obliged to monitor and ensure compliance with them.

1. Anti-virus software is used to protect against the operation of software aimed at obtaining unauthorized access to the IT system used to process personal data.
2. The AITS is responsible for planning and providing anti-virus protection, including ensuring the appropriate amount of licenses.
3. Each file loaded into an IT device, including an e-mail, is tested by the antivirus software.
4. In any IT device with Internet access, anti-virus software must be installed.
5. The virus definitions update takes place automatically by the system.

PROCEDURE FOR MAKING BACKUP COPIES

The following requirements for backing up of personal data processed in the Entity's IT system are established. The AITS is to ensure direct compliance to them.

1. Personal data processed in the IT system is secured via data backup.
2. The AITS is responsible for the establishment of the system that will store the backed-up personal data.
3. Backup copies of personal data in the IT system are made only by the AITS.
4. Backup copies are stored in places where they are protected against unauthorized takeover, modification, damage or destruction.
5. Backup copies should be controlled by the AITS periodically, in particular in terms of correctness of their execution and the possibility of reconstruction, by partial or complete reconstruction on dedicated computer equipment.
6. Devices containing copies of personal data processed in the IT system of the Entity are stored in a manner that prevents their loss, damage or access by unauthorized persons.
7. Backup copies are stored in a different location than the original of the secured data.
8. Backup copies are deleted immediately after their usefulness ceases.

PROCEDURE FOR INVENTORY OF EQUIPMENT AND DATA STORAGE MEDIA

The following requirements are established regarding the record of equipment and devices carrying the information for the processing of personal data in the Entity. The AITS is obliged to keep their register.

1. It is necessary to evidence all devices and storage media used to process personal data in the Entity, by entering them in a written register of devices and media used to process personal data (**Annex no. 15**).
2. Before allowing new devices and storage media to be used to process personal data at the Entity, they must be registered.
3. After removing the device or storage media used to process personal data in the Entity, it should be deleted from the Register of devices and storage media used for the processing of personal data.

PROCEDURE FOR REMOVING EQUIPMENT AND DATA STORAGE MEDIA

The following requirements regarding the removal of storage media for the processing of personal data in the Entity are established. The AITS is obliged to comply directly with them.

1. Storage media used to process personal data in the Entity shall be deprived of such data before being deleted, and then subjected to the procedure of at least three total overwriting.
2. In the case of the lack of possibilities described in the above item (eg. CDs, damaged hard drives) devices used to process personal data in the Entity, before being removed, are subjected to other activities resulting in permanent physical damage, making it impossible to read the data collected on the device.
3. After removing the device or data storage media used to process personal data in the Entity, it should be deleted from the Register of devices and storage media used for the processing of personal data.

PROCEDURE FOR SERVICE AND MAINTENANCE

The following requirements regarding the implementation of inspections, repairs and maintenance of the information system used for the processing of personal data are established. The purpose of the procedure is to ensure the continuity of the IT systems that process personal data and to protect personal data from unauthorized disclosure. The AITS is obliged to monitor and ensure compliance with them.

1. The inspections, repairs and maintenance of the IT equipment used to process personal data are carried out at the location of the Entity by the AITS, subject to the following conditions.
2. Repairs and maintenance of the IT equipment used to process personal data can be performed by enterprises or external contractors only on the basis of concluded agreements.
3. In the case of providing the IT equipment for the processing of personal data for repair:
    a. if the damage does not apply to the storage media, it should be removed and for the repair of the device should be given without the device on which personal data is stored,
    b. if the damage concerns the storage media it should be destroyed, and files containing personal data restored from the backup,
    c. if the damage concerns the storage media and at the same time there are no files containing personal data, then the repair should be carried out under the direct supervision of the authorized person or upon conclusion of the personal data entrustment agreement.
4. The AITS is obliged to perform random technical inspections of devices used to process personal data at least once a year.

The AITS maintains a register of repairs, inspections and maintenance of the IT system (**Annex o. 13**).

IV. GENERAL INSTRUCTIONS FOR PERSONS AUTHORIZED TO PROCESS PERSONAL DATA AND FOR APD / DPS / AITS

This manual is intended for all persons processing personal data in the entity, as well as for the APD and the DPS, as well as the AITS in the case of appointment.

DUTIES OF PERSONS AUTHORIZED TO PROCESS PERSONAL DATA

Each person is entitled to process personal data only after being authorized for doing that. The obligations of persons authorized to process personal data should be managed in accordance with the established internal regulations regarding the processing of personal data, in particular:

1. confidentiality of personal data and information on how to protect it, also after termination of employment or other civil law relationship,
2. non-use for private purposes the personal data, devices and programs used to process personal data in the Entity,
3. securing the area in which personal data are processed against access by unauthorized persons during the absence of persons authorized to process personal data using means provided by the APD,
4. ensuring that unauthorized persons are allowed to process personal data in the area of their processing only in the presence of a person authorized to process personal data and under his/her supervision,
5. informing about any suspected violation or noticed violations and weaknesses of the system processing personal data to the supervisor, who is obliged to inform the DPS,
6. immediately forwarding to the DPS all submissions regarding the processing of personal data by the Entity,
7. fulfillment of the information obligation in relation to persons whose personal data is processed by the Entity, if the authorized person is the person collecting the data,
8. use only programs and applications approved for use by the AITS or the APD,
9. protection of personal data and means of processing personal data against unauthorized access, disclosure, modification, destruction or distortion,
10. awareness and application of the Security Policy in part III and the provisions of the generally applicable law in the area of personal data protection, processed by the Entity.

Proceedings that are inconsistent with the above obligations may be considered by APD as a serious breach of employee duties within the meaning of art. 52 § 1 item 1 of the Labor Code or for breach of a civil law contract applicable between the parties of this agreement.

WHAT IS PERSONAL DATA?

Any information regarding an identified or identifiable natural person is considered to be personal data. In determining whether specific information is personal data, the Entity makes an individualized assessment, taking into account the specific circumstances and the type of means or methods needed in a given situation to identify the person.

An identifiable person is one whose identity can be identified directly or indirectly, in particular by reference to the personal identification number or one or more specific factors defining its physical, physiological, mental, economic, cultural or social characteristics. Personal data will be both data that allow the identification of the identity of a particular person, as well as those that do not allow for its immediate identification, but are, with a certain amount of costs, time and activities, sufficient to determine it.

WHEN CAN WE PROCESS REGULAR PERSONAL DATA?

The processing of personal data is permissible only if:

1. the data subject has agreed to the processing of his/her personal data in one or more specific purposes,

2. processing is necessary for the performance of a agreement to which the data subject is a party, or to take action at the request of the data subject, before concluding the agreement,
3. processing is necessary to fulfill the legal obligation imposed on at the APD,
4. when processing is necessary to protect the vital interests of the data subject or another natural person,
5. when processing is necessary to perform a task carried out in the public interest or within the exercise of public authority entrusted to the APD,
6. when processing is necessary for purposes deriving from legitimate interests pursued by the APD or by a third party, except when the interests or fundamental rights and freedom of the data subject have overriding effect on those interests, requiring the protection of personal data in relation to those interests, prevail over those interests particularly when the data subject is a child.

WHEN CAN WE PROCESS "SENSITIVE" PERSONAL DATA?

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

1. the data subject has expressly consented to the processing of such personal data for one or more specific purposes, unless the EU or Member State law provides that the data subject may not derogate from the prohibition,
2. processing is necessary to fulfill the obligations and exercise specific rights by the controller or data subject in the field of the Labor Law, social security and social protection,
3. processing is necessary to protect the vital interests of the data subject or another natural person and the data subject is physically or legally incapable of giving consent,
4. processing is carried out within the framework of legitimate activities carried out with appropriate safeguards by the foundation, association or other non-profit entity with political, ideological, religious or trade objectives, only if processing relates solely to members or former members of that Entity or persons maintaining permanent contacts with it for its purposes and that personal data is not disclosed outside that Entity without the consent of the data subject,
5. processing relates to personal data that is obviously made public by the data subject,
6. processing is necessary for the establishment, investigation or defense of claims or in the administration of justice by the court,
7. processing is necessary for reasons relating to major public interests under the EU law or the law of a Member State which are proportionate to the objective pursued, does not affect the substance of the right to data protection and provides for appropriate and specific measures to protect fundamental rights and the interests of the person the data concern,
8. processing is necessary for the purpose of occupational health or occupational medicine, for the assessment of the employee's ability to work, medical diagnosis, provision of health care or social security, treatment or management of health and social security systems or services under the EU law or the law of a Member State,
9. processing is necessary for reasons relating to the public interest in the field of public health, such as protection against serious trans-border threats to health or ensuring high standards of quality and safety of healthcare

and medicinal products or medical devices, under the EU law or the law of a Member State, which provide for appropriate concrete measures to protect the rights and freedom of data subjects, in particular professional secrecy,

10. processing is necessary for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, on the basis of the EU law or the law of a Member State that are proportionate to the objective pursued, does not infringe the essence of the right to data protection and provide for appropriate, specific measures to protect fundamental rights and the interests of the data subject.

PRINCIPLES OF PERSONAL DATA PROCESSING

The Entity performs its duties by applying special diligence to protect the interests of the data subjects, ensuring that the data is:

1. **Processed in accordance with the law.**
   I.e. comply with all legal standards, both those already existing at the time of initial enforcement of the EU Regulation and those that were later introduced into the legal order. Compliance with the law applies to keeping both substantive law and procedural rules.

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

3. **Substantially correct and adequate in relation to the purposes for which they are processed.**
   I.e. information resulting from the data processed by the APD is truthful, complete and corresponds to the current state of affairs. The APD processes data only to the extent that it is necessary to fulfill the purpose for which data is processed by him/her.

4. **Stored in a form that permits the identification of persons whom they concern, for no longer than it is necessary to achieve the purpose of processing.**

5. **The APD applies technical and organizational measures ensuring protection of personal data being processed, appropriate to threats and categories of protected data**.

   In particular, the APD should protect data from being made available to unauthorized persons, being taken away by an unauthorized person, processed in violation of generally applicable laws and changes, loss, damage or destruction.

In addition, the Entity ensures the security of personal data being processed, in particular by:

1. **Confidentiality of personal data.**
   I.e. personal data is not shared or disclosed to unauthorized persons, and unauthorized persons have no access to personal data.
2. **Integrity of personal data.**
   I.e. personal data is complete and unchanged in an unauthorized way.
3. **Accountability of activities on personal data.**
   I.e. all relevant activities performed in the processing of personal data have been recorded and it is possible to identify the person who performed the action.

OBLIGATIONS FOR PROCESSING DESIGNING

The existing rules for the protection of personal data should be already taken into account at the stage of designing and developing data processing methods, and also at every subsequent processing stage.

In particular, it is necessary to ensure the following rules:

- minimizing the processing of personal data,
- the fastest possible pseudonymisation of personal data,
- transparency regarding the function and processing of personal data,
- enabling the data subject to monitor data processing,
- enabling the APD to create and improve protection means.

The APD's duties include ensuring that the solutions applied comply with the provisions of the Regulation and protection of the rights of the persons of which the data is processed. However, authorized persons, when performing official duties, should have this principle in mind.

OBLIGATIONS OF DEFAULT PRIVACY KEEPING

The obligation to implement default privacy settings should be taken into account even at the stage of designing and developing data processing methods, and also at every subsequent processing stage.

Its essence is the implementation by the APD of appropriate technical and organizational measures so that by default only the personal data which is essential will be processed to achieve each specific purpose of processing.

This obligation refers to the amount of personal data collected, the scope of their processing, the period of their storage and their availability. In particular, these measures ensure that by default personal data were not made available without the intervention of a person in charge to unspecified number of natural persons.

This policy means that the privacy settings used by the data administrator are to have the maximum protection of the users.

Implementation of the principle of default data protection is tantamount to the need for users to take additional steps in case they wants to limit their privacy in any way, e.g. by making their data available to more individuals.

Thus, the change in the default maximum protection of privacy will only occur at the explicit request of the users of the system or software.

PROCEDURE FOR IMPLEMENTING THE INFORMATION OBLIGATION IN CASES OF PERSONAL DATA COLLECTION

In the case of collecting personal data, it is usually necessary to provide information clearly in accordance with the disclosure requirements template (**Annex no. 1**).

With respect to the data collection processes from the persons they concern, the rules set out in the Annex shall not apply if the provision of another act allows the data to be processed without disclosing the actual purpose of their collection or if the data subject already has this information.

With regard to the data collection processes not from the persons to whom they relate, the rules set out in the Annex shall not apply if:

1. the provision of another law provides or permits the collection of personal data without the knowledge of the data subject,
2. informing requires a disproportionate effort - in particular, when the data is processed for archiving, statistical and research purposes,
3. passing the information proves impossible,
4. the recording or disclosure of data is expressly required by the EU or national law, concerns professional secrecy arising from the EU law or national law.

PROCEDURE FOR ENTRUSTING OF PERSONAL DATA PROCESSING

In case of the need to process personal data by separate entities providing services for the APD, he/she may entrust its processing.

Entrusting is not about sharing data. Sharing is the transfer of data to another entity (recipient of data), which becomes their APD in the intention of achieving his/her own goals. Entrusting consists of the data being processed by the receiving entity in the intent to implement the APD's objectives. Entrusting is, for example, disclosing personal data to an external accounting office. The disclosure is usually, for example, disclosure of personal data to the Tax Authorities.

Entrusting the processing of personal data takes place on the basis of a contract or other legal instrument that is subject to the EU law or the law of a Member State and bind the processing entity and the APD, specify in particular the subject and duration of processing, the nature and purpose of the processing, the type of personal data and categories of persons, where the data pertain, the responsibilities and rights of the administrator.

It is recommended to use the contract template for entrusting personal data (**Annex no. 16**).

In case when a different standard agreement is used, different from the template of the agreement at the disposal of the APD, it is necessary to verify in detail the compliance of this other standard with the provisions of the generally applicable law, in particular the GDPR.

The APD may maintain a document of the register of entities to which the Entity entrusts personal data (**Annex no. 17**).

PROCEDURE FOR THE ACCEPTANCE OF ENTRUSTED PERSONAL DATA

An entity acting as a processing entity (processor) may accept personal data entrusted to it by separate APDs for processing.

Entrusting the processing of personal data takes place on the basis of an agreement or other legal instrument that is subject to the EU law or the law of a Member State and bind the processor and the APD, specify in particular the subject and duration of processing, the nature and purpose of the processing, the type of personal data and categories of persons, where the data pertain, the responsibilities and rights of the administrator.

The entity may use the agreement template for entrusting personal data (**Annex no. 16**).

In case when a different standard agreement is used, different from the template agreement at the disposal of the Entity, it is necessary to verify in detail the compliance of this other standard with the provisions of the generally applicable law, in particular the GDPR.

The Entity may keep a register of categories of personal data processing activities on behalf of the administrator - a processor register (**Annex No. 4**).

The exclusion of the obligation of keeping the category register of processing activities applies in the cases specified in art. 30 item 5 of the EU Regulation.

Entrusting is not about sharing data. Sharing is the transfer of data to another entity (recipient of data), which becomes its APD, yet entrustment consists of the processing of data by an entity that is not APD of said data**.**

PROCEDURE FOR THE CIRCULATION OF PERSONAL DATA

Sharing personal data is one of the forms of its processing. Sharing personal data can be defined as any activities that allow entities other than APD to become familiar with it, with the exception of the above-mentioned entrustment. Sharing does not refer to the employees of the Entity, which act on the basis of granted authorizations.

1. It is not important whether the sharing of data is paid or not, so that the activity is considered as circulation.
2. It is irrelevant whether the circulating takes place in the form of an oral or written transmission, by means of the media or via a computer network, etc., so that the act is considered as circulation.
3. The circulation of personal data to persons or entities authorized to receive it is carried out on the basis of the law.
4. Circulated personal data may be used only for the purpose for which it has been circulated.

The APD or a person authorized by him/her may keep a document of the register of entities to which the Entity makes personal data available (**Annex no. 18**). The document contains information on circulation personal data for all entities, excluding:

1. persons or entities entrusted with personal data,
2. persons authorized to process personal data,
3. data subjects.

PROCESS OF PROCESSING OF DATA IN PAPER FORM

The following procedure for processing of personal data in paper form is established.

1. Personal data in paper form may be on desks only for the time necessary to perform business activities and then they must be stored in locked cabinets.
2. There should not remain on desks documents containing personal data of other people than at the time being served.
3. When leaving the desk, documents never to be left unattended.
4. After finishing work, the documents should be secured in a locked cabinet.
5. No unnecessary printouts are to be stored.
6. Unnecessary printouts and other conventional documents (on paper) containing personal data should be destroyed in a document shredder.
7. The person who processed the data is responsible for the proper destruction of unnecessary paper documents containing personal data.

Supervision over the proper destruction of documents containing personal data is exercised by the DPS.

PROCEDURE FOR HANDLING ACCESS PASSWORDS AND FILES PROTECTED BY PASSWORDS

Each authorized person is obliged to protect his/her access data to the IT systems used to process personal data. The scope of access data is included in particular:

1. access passwords,
2. software keys (files enabling access - e.g. certificates to VPN),
3. hardware keys,
4. other mechanisms enabling access to the IT systems.

Basic methods of protection of data access:

1. not providing of data access to other people (e.g. transferring your access password to third parties),
2. not storing data access in public places (e.g. writing or saving access passwords in easily accessible places),
3. protection of data access prior to acquisition by third parties.

PROCEDURE FOR USING INTERNET

The following procedure for using Internet in the Entity is established:

1. The IT system users have the right to use Internet only for the purpose of performing their official duties.
2. It is prohibited to use the options of auto-completing forms and remembering passwords in the web browser settings.
3. It is forbidden to save data onto storage media devices used in the IT hardware and run any programs or applications not approved for use by the AITS.
4. It is prohibited to run files downloaded without scanning by the antivirus program or marked by this program as dangerous or potentially dangerous.
5. It is prohibited to send personal data using unencrypted websites. For this purpose, before sending the data, it is necessary to check whether the information about the appropriate security is visible in the address bar of the website (green padlock, https protocol).
6. It is prohibited to send personal data to countries outside the EEA (European Economic Area, which covers all European Union countries, Iceland, Liechtenstein and Norway), without the prior consent of the DPS.
7. When using the internet, users of the IT system are required to observe industrial property rights and copyrights.

PROCEDURE FOR USING E-MAIL

The following procedure for using e-mail in the Entity is established:

1. Do not open attachments (files) in electronic correspondence sent by an unknown sender. This possibility is allowed only after a positive verification of the sender's e-mail address (e.g. when we find out that it is a customer of the Entity). In other cases, a message should be sent to the AITS who can verify the safety of the attachment.
2. When sending any e-mails to many recipients, use the BCC function to hide the recipients' e-mail addresses. In this case, the e-mail addresses of the addressees should be entered in the BCC line, and as its recipient enter, for example, your own e-mail address.

3. In case of sending any personal data via e-mail, cryptographic mechanisms should be used (e.g. file compression and password protection of attached files). In this case, the access password to the file should be sent by another means of communication (e.g. via telephone text message).
4. Before sending a message containing personal data, the recipient's e-mail address must be verified at least once.
5. In case of detection of the appearance of malicious software or finding disturbances in the functioning of the IT system, the authorized person is obliged to notify AITS about this fact.
6. It is recommended that when sending personal data by e-mail, include in the content a request for acknowledgment of receipt and readout by the addressee.

PROCEDURE FOR USING PORTABLE DEVICES

The following procedure for the use of portable devices (e.g. laptops, smartphones) is set up in the Entity:

1. Before starting the processing of personal data, an authorized person should check if there are no signs of physical security breaches. In case of any irregularities, notify the AITS.
2. An authorized person is obliged to notify the AITS of an attempt to log into the IT system used to process personal data by an unauthorized person.
3. When commencing work with a device used to process personal data, the authorized person is obliged to enter his/her access password or unlock the device by using biometric data.
4. It is forbidden to perform any operations in the IT system used to process personal data by using the identifier, access password or biometric data of another authorized person.
5. The settings of displays or monitors of mobile devices must ensure limiting the possibility of viewing the displayed data to third parties.
6. The authorized person is required to exercise due diligence in order to prevent unauthorized third parties from viewing information including personal data processed within the system that is displayed on the device's screen.
7. If it is necessary to interrupt or terminate work on a mobile device used to process personal data, you should block access to this device.
8. Portable computers may be taken from the place of processing of personal data only in special cases, after informing the AITS or the competent authorized person. This item does not apply to authorized persons who perform activities outside the Entity's location as part of their official duties.
9. A person using a mobile device used to process personal data shall be particularly careful during its transport, storage and use outside of the Entity's location.
10. It is forbidden to leave mobile devices for the processing of personal data without supervision, outside the location of the Entity.
11. It is forbidden to log into open networks (hotspots, open Wi-Fi) using mobile devices used to process personal data.
12. It is forbidden to take portable devices used to process personal data to countries outside the EEA (European Economic Area, which covers all countries of the European Union, Iceland, Liechtenstein and Norway) without the prior consent of the DPS or the APD.
13. It is forbidden to disable antivirus programs and prevent backups from being made by the IT system.
14. In the case of finding the appearance of malicious software or finding disturbances in the functioning of the IT system used to process personal data, the authorized person is obliged to notify the AITS about this fact.

15. Backup copies of personal data in the IT system are performed only by the AITS.

PROCEDURE FOR USING STATIONARY COMPUTERS

The following procedure for using desktops in the Entity is established:

1. Before starting the processing of personal data, an authorized person should check if there are no signs of physical security breaches. In the event of any irregularities, notify the AITS.
2. An authorized person is obliged to notify the AITS of an attempt to log into the IT system used to process personal data by an unauthorized person.
3. When commencing work with a computer used to process personal data, the authorized person is obliged to enter his/her access password or unlock the computer by using biometric data.
4. It is forbidden to perform any operations in the IT system used to process personal data by using the identifier, access password or biometric data of another authorized person.
5. The settings of desktop monitors must ensure that the displayed data can not be viewed by third parties.
6. The authorized person is obliged to exercise due diligence in order to prevent unauthorized third parties from accessing information including personal data processed within the system, which are displayed on the computer screen.
7. If it is necessary to interrupt or terminate work on a desktop computer used to process personal data, you should block access to this computer.
8. It is forbidden to take desktops out of the Entity's location.
9. It is forbidden to disable antivirus programs and prevent backups from being made by the IT system.
10. Backup of personal data in the IT system is performed only by the AITS.

PROCEDURE FOR SERVICE AND MAINTENANCE

The following requirements regarding the implementation of inspections, repairs and maintenance of the information system used for the processing of personal data are established:

1. The AITS is responsible for the inspections, repairs and maintenance of the IT equipment used to process personal data.
2. If there is a need to carry out repair or maintenance of the IT equipment used to process personal data, the authorized person is obliged to report this fact to the AITS.
3. An authorized person is obliged to make the IT equipment available for the purpose of performing the inspection, maintenance or repair by the AITS.
4. It is forbidden to carry out reviews and maintenance of the IT systems used to process personal data and information media devices used to process personal data independently by employees.
5. In case of remote repair, in particular by using the means of teletransmission of the screen of the person authorized to process data by the AITS, before commencing this operation the authorized person is obliged to close any programs for processing of personal data, the use of which is not necessary during the performance of these activities.

PROCEDURE IN CASE OF VIOLATION OF DATA PROTECTION RULES FOR PERSONS AUTHORIZED TO PROCESSING PERSONAL DATA

A breach of personal data protection is a security breach leading to accidental or unlawful:

- damage,
- loss of,
- modification,
- unauthorized disclosure or
- unauthorized access to personal data,

sent, stored or otherwise processed. In case of a breach of personal data protection, the infringement procedure described below should be started.

In case of a suspected violation of personal data protection rules, every person authorized to process personal data is obliged immediately:

1. inform the DPS or the APD about this fact via e-mail or IPW,
2. until receiving feedback, refrain from starting or continuing work, as well as taking any action that may cause blurring of traces of the violation or other evidence,
3. if possible, protect elements of the information system or files, mainly by preventing unauthorized access to them.

Afterwards you should expect documented feedback from the informed person.

V. FINAL PROVISIONS

1. The security policy is a document in force at the Entity in the scope of implementation, observance and verification of personal data protection rules.
2. The security policy is a document valid for all persons admitted to the processing of personal data as part of the Entity's activities.
3. Every person admitted to the processing of personal data within the Entity's activity is required to read this Security Policy.
4. Violation of the principles resulting from the Security Policy may constitute grounds for instituting disciplinary proceedings against the offender.
5. Initiating or conducting disciplinary proceedings against a person who violates the principles resulting from the Security Policy does not exclude the possibility of instituting criminal proceedings and pursuing claims by civil action.
6. The security policy together with the annexes shall enter into force on the day of signing by the APD.
7. In matters not covered by the Security Policy, generally applicable provisions of law, in particular the EU Regulation, apply.

VI. ANNEXES

The annexes to this Security Policy form a part of it, subject to supplementation:

1. Disclosure requirements template (Annex no. 1),
2. Risk analysis template (Annex no. 2),
3. Register of personal data processing activities (Annex no. 3),

4. Register of categories of processing activities performed on behalf of the administrator (Annex no. 4),
5. Template of authorizations for processing personal data by employees (Annex no. 5),
6. Template of authorizations for processing personal data by persons employed on the basis of civil law contracts (Annex no. 6),
7. Register of employees authorized to process data (Annex no. 7),
8. Register of persons employed under a civil law agreements authorized to process data (Annex no. 8),
9. Template of the declaration on appointing the Data Protection Supervisor (Annex No. 9),
10. Template of the assessment of the effects of planned processing operations for the protection of personal data (Annex no. 10),
11. Template for reporting a data protection breach to POPDP (Annex no. 11),
12. Registry of personal data safety violations (Annex no. 12),
13. Register of repairs, inspections and maintenance of the IT system (Annex no. 13),
14. Register of activities in the IT system (Annex no. 14),
15. Register of devices and media used to process personal data (Annex no. 15),
16. Template for entrusting personal data (Annex no. 16),
17. Register of entities entrusted with personal data (Annex No. 17),
18. Register of entities to which the Entity makes personal data available (Annex no. 18).

Signature of the Personal Data Administrator	Date