PERSONAL DATA PROTECTION POLICY

Oddsee Sp. z o. o

UL. Jana z Kolna 11,

80-864 Gdańsk

Date of introduction:	2/11/2022
Version:	1
Update dates:	02/11/2022
Compiled by:	[Daria Jendrzejewska, attorney-at-law]
Approved by:	[Szymon Kot, President of the Management Board]

CONTENTS

A. GENERAL INFORMATION

1. PURPOSE OF THE PERSONAL DATA PROTECTION POLICY

The personal data protection policy has been developed and implemented in the structure of the Data Administrator in order to ensure compliance of the processing of personal data with the requirements of Polish and European legal acts in force in this regard, in particular:

1. 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 regulation on data protection) ,
2. The Act of May 10, 2018 on the Protection of Personal Data (consolidated text, Journal of Laws of 2018, item 1000, as amended).

The personal data protection policy applies to all employees of the Data Administrator who, in the scope of their official duties, process personal data, as well as other persons who, under the Data Administrator's authorization, have gained access to personal data. Each of these persons has been familiarized with the most important data security procedures described in the Personal Data Protection Policy and has been obliged to comply with them to the extent resulting from the assigned tasks. The persons in question made a statement that they had read the data security procedures and undertook to use them.

Any doubts regarding the interpretation of the provisions of the Personal Data Protection Policy should be resolved in favor of ensuring the highest possible level of personal data protection and the implementation of the rights of data subjects.

2. TERMINOLOGY

1. **Data Administrator (ADO)** - [Oddsee Sp. z o. o.],
2. **Information Systems Administrator (ASI)** - a person appointed by the Data Administrator, coordinating activities related to ensuring the security of IT systems, including responsible for supervision over the protection of personal data processed in IT systems used by the Data Administrator,

3. **personal data** - information about an identified or identifiable natural person ("data subject"), where an identifiable natural person is understood as a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name and surname , identification number, location data, internet identifier or one or more specific factors determining the physical,

---

physiological, genetic, mental, economic, cultural or social identity of a natural person,

4. **DPIA** - *data protection impact assessment* ,

5. **Data Protection Officer (DPO) -** a person appointed by the Data Administrator, coordinating the processes related to compliance with the principles of personal data protection as part of the personal data processing processes taking place in the Data Administrator's structure,

6. **supervisory authority** - an independent public authority to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data in the Union, established in each EU Member State, whose primary task is to monitor the application of the GDPR,

7. **third country** - a country not belonging to the European Economic Area.

8. **third country** - a country not belonging to the European Economic Area.

9. **processor** - a natural or legal person, public authority, entity or other entity that processes personal data on behalf of the Data Administrator,

10. **Policy** - this Personal Data Protection Policy,

11. **employee** - a person cooperating with the Data Administrator on the basis of an employment contract or a civil law contract,

12. **processing** - an operation or a set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, organizing, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, distributing or otherwise sharing, adjusting or combining, limiting, deleting or destroying,

13. **GDPR** - 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 regulation on the protection of data),

14. **Union** - European Union,

15. **Act** - the Act of May 10, 2018 on the protection of personal data (uniform text in Journal of Laws of 2018, item 1000 as amended),

3. THE SCOPE OF INFORMATION COVERED BY THE PERSONAL DATA PROTECTION POLICY AND THE SCOPE OF APPLICATION

The personal data protection policy describes the rules and procedures for the processing of personal data. It is a set of rights, rules and practical experiences regarding the management, protection and distribution of personal data within the Data Administrator. The policy relates as a whole to the problem of securing personal data, i.e. both to securing traditionally processed data and data processed in IT systems.

The personal data protection policy applies to all activities that constitute, in accordance with the GDPR, the processing of personal data. Regardless of the source of personal data, their scope, purpose of collection, method of processing or processing time, the principles included in the Policy are applied.

The Rigor of the Policy also applies to data entrusted to the Data Administrator for processing on the basis of a contract for entrusting the processing of personal data or another legal instrument, as well as personal data that has been made available to the Data Administrator.

B. PERSONS RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA

1. THE STRUCTURE OF THE ORGANIZATION OF PERSONAL DATA PROTECTION

The following are responsible for the processing of personal data and their protection in accordance with the provisions of the GDPR, the Act, the Policy and internal procedures in the field of personal data protection implemented in the Data Administrator's structure:

1. Data Administrator,
2. Persons authorized to process personal data.

1.1. A DATA ADMINISTRATOR

1. The Data Administrator is responsible for:
   a) ensuring appropriate organizational and technical measures to ensure and demonstrate the processing of personal data in accordance with the principles of personal data processing set out in the GDPR,
   b) implementation of appropriate personal data protection procedures,
   c) if it deems it necessary, the use of approved codes of conduct or approved certification mechanisms, as an element to determine compliance by the Data Administrator with its obligations,
   d) providing measures enabling the correct implementation of the rights of data subjects,
   e) keeping a register of personal data processing activities,
   f) keeping a register of processing categories carried out on behalf of another administrator,
   g) cooperation with the supervisory authority in the performance of its tasks,
   h) implementation of appropriate organizational and technical measures to ensure a level of security corresponding to the existing risk of violating the rights or freedoms of data subjects,

i) reporting a breach of personal data protection to the competent supervisory authority, and in the event of appropriate grounds, also to the data subject,

j) documenting any breaches of personal data protection, including the circumstances of the breach, its effects and the remedial actions taken,

k) ensuring appropriate measures to assess the effects of the planned processing operations on the protection of personal data in a situation where a given type of processing may result in a high risk of violating the rights or freedoms of natural persons, including, if there are appropriate grounds, consultation with the supervisory authority,

l) granting authorizations to process personal data and keeping records of persons authorized to process personal data,

m) ensuring the legality of the transfer of personal data to third parties.

1.2. I N DATA PROTECTION OFFICER

1. Due to the fact that the Administrator does not meet the criteria obliging him to appoint a Data Protection Officer, at the present stage of advancement of the Administrator's undertaking, the appointment of a DPO is withdrawn. The administrator will appoint the Data Protection Officer after the project reaches the stage of development related to the mass processing of personal data.

2. Specimen documents of appointment and appeals of the DPO can be found in Annex 11 to the Policy.

3. The DPO will be appointed by the Data Administrator on the basis of professional qualifications, in particular expertise in data protection law and practices, and the ability to fulfill their tasks.

4. The tasks of the DPO will include:

   4.1. informing about the obligations arising from the GDPR and other relevant EU or Member State regulations on the protection of personal data and advising in this regard,

   4.2. monitoring compliance with the GDPR and other relevant EU or Member State legislation on the protection of personal data,

   4.3. monitoring compliance with the implemented personal data protection procedures,

   4.4. advice on the division of duties (e.g. between co-administrators, the Data Administrator and the processor or between the employees of the Data Administrator),

   4.5. activities increasing the awareness of employees of the Data Administrator in the scope of obligations arising from the GDPR or adopted procedures,

   4.6. training for employees of the Data Administrator participating in data processing operations,

   4.7. conducting audits in the field of compliance with the GDPR and implemented personal data protection procedures,

   4.8. upon request, providing recommendations as to the impact assessment for the protection of personal data and monitoring its implementation,

   4.9. cooperation with the supervisory authority and acting as a contact point for the supervisory authority in matters related to data processing,

4.10. acting as a contact point for data subjects in all matters related to the processing of their personal data and the exercise of their rights under the GDPR .

5. Until the DPO is appointed, the above-mentioned tasks are performed by the Data Administrator.

1.3. A ADMINISTRATOR OF INFORMATION SYSTEMS

1. At the present stage of advancement of the project, the Administrator refrains from appointing the IT Systems Administrator. The administrator will appoint ASI after the project reaches the stage of development related to the mass processing of personal data via the IT system.
2. The ASI function will be performed by a person appointed by the Data Administrator.
3. The templates of the ASI designation documents and appeals can be found in Annex 12 to the Policy.
4. The tasks of ASI will include:
    - 3.1. keeping a register of granted authorizations to IT systems,
    - 3.2. developing and updating Annex 10 to the Policy, which is a general description of technical security measures implemented in the structure of the Data Administrator,
    - 3.3. supervision over the application of measures ensuring the security of personal data processing in IT systems, in particular preventing unauthorized access to these systems,
    - 3.4. taking appropriate action in the event of detecting violations in the security system,
    - 3.5. identification and analysis of threats and risk assessment to which the processing of personal data in IT systems may be exposed,
    - 3.6. exercising supervision over backups;
    - 3.7. initiating and supervising the implementation of new tools, organizational procedures and methods of managing IT systems, which are to lead to the strengthening of security in the processing of personal data,
    - 3.8. undertaking other activities in the field of securing data processing in IT systems,
    - 3.9. carrying out periodic reviews of the validity and application of procedures in the field of data processing in IT systems, based on the prepared review plan.
    - 3.10. close cooperation with the DPO or the Data Administrator in the field of security and rules for the processing of personal data in IT systems.

4. Until ASI is appointed, the above-mentioned tasks are performed by the Data Administrator.

1.4. PERSONS AUTHORIZED TO PROCESS PERSONAL DATA

1. Each person who has been authorized to process data is obliged to protect it in a manner consistent with the provisions of the GDPR, the Act and the provisions of the Policy.

2. The authorized person is obliged to keep the personal data and the methods of their protection confidential. This obligation also exists after the termination of employment. The relevant provision on the acceptance of the obligation to keep the processed personal data secret includes the authorization, the specimen of which is in Annex 2 to the Policy.

3. Violation of the obligation to protect personal data, and in particular the obligation to keep personal data secret, results in incurring criminal liability under the provisions of the Act and constitutes a serious breach of employee obligations and may be the basis for termination of the employment relationship pursuant to Art. 52 of the Act of June 26, 1974, the Labor Code (consolidated text, Journal of Laws of 2018, item 108, as amended), or termination of the civil law relationship.

C. RULES FOR THE PROCESSING OF PERSONAL DATA

1. GENERAL RULES FOR THE PROCESSING OF PERSONAL DATA

1. The processing of personal data in the structure of the Data Administrator takes place in accordance with the general rules for the processing of personal data specified in art. 5 GDPR. This means that personal data is processed:

1.1 in accordance with the law, based on at least one prerequisite for the legality of the processing of personal data indicated in art. 6 or 9 GDPR (*legality principle*),

1.2 in a reliable manner, taking into account the interests and reasonable expectations of data subjects (the *principle of fairness*),

1.3 in a transparent manner for data subjects (*transparency principle*),

1.4 for specific, explicit and legitimate purposes (*the purpose limitation principle*),

1.5 to the extent adequate, relevant and necessary for the purposes for which they are processed (the *principle of data minimization*),

1.6 taking into account their correctness and possible updating (*the principle of correctness*),

1.7 for a period not longer than it is necessary for the purposes for which they are processed (*principle of storage limitation*),

1.8 in a manner that ensures appropriate security (*integrity and confidentiality*).

2. Data Administrator guarantees that certain decisions relating to the processing of personal data have been analyzed from the point of view of compliance with the general principles of data processing, and above all, that they are consistent with them.

2. THE SCOPE OF PERSONAL DATA PROCESSED

1. The policy applies to all personal data processed by the Data Administrator, regardless of the form of their processing (electronic or paper) and whether they are data processed in data sets, in sets or they constitute individual personal information.

2. The list of personal data files, the administrator of which is the Data Administrator, and the processing processes taking place in these files, is attached as Appendix 1 to the Policy.

3. The Data Administrator runs:

   3.1. register of personal data processing activities, of which he is the administrator,

   3.2. a register of the categories of processing activities carried out on behalf of the administrators who entrusted him with data processing.

4. The register referred to in point 3.1. contains at least the following information:

   4.1. the name and contact details of the Data Administrator and any joint controllers,

   4.2. where applicable, the name and contact details of its representative,

   4.3. name and surname and contact details of the IOD, in the event of his appointment,

   4.4. the purposes of the processing,

   4.5. description of the category of data subjects,

   4.6. description of the category of personal data,

   4.7. categories of recipients to whom personal data have been or will be disclosed, including recipients in third countries or in international organizations,

   4.8. where applicable, the transfer of personal data to a third country or an international organization, including the name of that third country or international organization, and in the case of transfers referred to in art. 49 sec. 1, second paragraph of the GDPR, documentation of appropriate security measures,

4.9. if possible, the planned dates of deletion of individual data categories, 4.10. a general description of the technical and organizational security measures.

5. The register referred to in point 3.2. contains at least the following information:

5.1. name and contact details of the Data Administrator,

5.2. name and surname or name and contact details of each administrator on behalf of which the Data Administrator acts,

5.3. where applicable, the name and contact details of a representative of each administrator on behalf of which the Data Administrator acts,

5.4. where applicable, the name and contact details of the DPO of each administrator on behalf of which the Data Administrator acts,

5.5. the categories of processing performed on behalf of each of the controllers,

5.6. where applicable, the transfer of personal data to a third country or an international organization, including the name of that third country or international organization, and in the case of transfers referred to in art. 49 sec. 1, second paragraph of the GDPR, documentation of appropriate security measures,

5.7. a general description of the technical and organizational security measures.

6. The Data Administrator keeps the registers referred to in point 3 in electronic form.

7. In the event of a request by the supervisory authority in this regard, the Data Administrator provides him with the registers kept by him.

3. D LEAVING PEOPLE TO PROCESS PERSONAL DATA

1. The Data Administrator, implementing the Policy, in the scope of sharing personal data within its own (internal) structure, allows their processing in an IT system or in a paper version only to persons who have obtained prior, appropriate authorization to process personal data.

2. Authorization to process personal data is granted after training or familiarizing the authorized person with the rules of personal data protection in force in the Data Administrator's structure in another form.

3. Authorization to process personal data is granted individually, with a clear indication of what data sets it covers.

4. The Data Administrator keeps a register of persons authorized to process personal data, a template of which is attached as Annex 4 to the Policy.

5. The detailed procedure for training and granting authorizations to process personal data is attached as Appendix 3 to the Policy.

4. ENTRUSTING THE PROCESSING OF PERSONAL DATA

1. By implementing the Policy, the Data Administrator allows the personal data of which he is the administrator to be processed outside his own organizational structures. This may only take place by entrusting data, for a specific purpose and scope, to a processor under a contract for entrusting the processing of personal data or another legal instrument.

2. The basic condition for the admissibility of entrusting data processing on behalf of the controller is subjecting the planned outsourcing to an analysis which should ensure that the selection of the processor depends on the provision of sufficient data protection guarantees.

3. The contract for entrusting the processing of personal data concluded by the Data Administrator must comply with the provisions of art. 28 of the GDPR, i.e. in particular to specify:

   3.1. the subject of entrustment,

   3.2. duration of the entrustment,

   3.3. nature and purpose of processing,

   3.4. type of entrusted personal data,

   3.5. categories of data subjects,

   3.6. conditions for subcontracting data processing 3.7. obligations and rights of the Data Administrator ,

   3.8. the obligations of the processor.

4. The entrustment agreement may be concluded in writing, including electronic.

5. If the elements of entrusting data processing indicated in point 3 are already included in the contract concluded with a given entity, there is no need to draw up an additional contract for entrusting the processing of personal data.

6. The Data Administrator is responsible for concluding contracts for entrusting the processing of personal data.

7. The contract for entrusting the processing of personal data is signed in accordance with the rules of representation of the Data Administrator or granted powers of attorney.

8. Each entrustment of personal data must be obligatorily entered in the register of personal data processing activities.

9. The Data Administrator has the right to control the processing entities entrusted with the processing of personal data.

10. The Data Administrator, in the scope of his business, may also process personal data entrusted by entities for which he provides services. Acceptance of data for entrustment by the Data Administrator must be obligatorily recorded in the register of categories of personal data processing activities.

5. ACCESS TO PERSONAL DATA

1. By implementing the Policy, the Data Administrator allows the personal data of which he is the administrator to be transferred to other administrators in the form of data sharing.
2. The disclosure of personal data may take place only on the basis of at least one of the conditions indicated in art. 6 GDPR and / or Art. 9 GDPR.
3. Entities or categories of entities to which personal data are disclosed must be obligatorily indicated in the register of personal data processing activities.

6. TRANSFERRING PERSONAL DATA TO THIRD COUNTRIES

1. The transfer of data, the administrator of which is the Data Administrator, to third countries and international organizations may only take place under the conditions provided for in Chapter V of the GDPR.

2. The transfer of data to third countries may take the form of both entrusting the processing of personal data and providing personal data, which means that depending on the type of transfer, the provisions of sub-chapters 4 and 5 of the Policy should also be taken into account.

3. The transfer of personal data, the controller of which is the Data Administrator, to a third country may take place if the European Commission has issued a decision that a given third country, territory or specific sector or specific sectors in that third country or a given international organization ensures an adequate level of protection. Such transfer does not require special authorization.

4. In the absence of a decision of the European Commission, referred to in point 3, the transfer of personal data to a third country is possible if the Data Administrator independently provides appropriate security and provided that enforceable rights of data subjects and effective legal remedies will apply. . The Data Administrator may provide appropriate security by means of: 4.1. a legally binding and enforceable instrument between public authorities or entities,

   4.2. binding corporate rules approved by the supervisory authority, applicable to each member of a group of companies or a group of entrepreneurs engaged in a joint economic activity,

   4.3. standard data protection clauses adopted or approved by the European Commission,

   4.4. standard data protection clauses adopted by a supervisory authority and approved by the European Commission,

   4.5. an approved code of conduct together with binding and enforceable obligations of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, or

   4.6. an approved certification mechanism together with binding and enforceable obligations of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

5. Subject to the authorization of the competent supervisory authority, appropriate safeguards referred to in point 4 may be provided by the Data Administrator, in particular by means of:

5.1. contractual clauses between the Data Controller or processor and the Data Controller, processor or recipient of personal data in a third country or international organization, or

5.2. provisions of administrative arrangements between public authorities or bodies that provide for enforceable and effective rights of data subjects.

6. In special cases, it is allowed to transfer personal data by the Data Administrator to a third country despite the lack of a decision of the European Commission referred to in point 3 and ensuring appropriate safeguards referred to in points 4 and 5. These special cases include the transfer of data under provided that:

6.1. the data subject, informed of the possible risks that may be associated with the proposed transfer, expressly consent to it,

6.2. the transfer is necessary for the performance of the contract concluded with the data subject,

6.3. the transfer is necessary to conclude or perform a contract concluded in the interest of the data subject,

6.4. the transfer is necessary for important reasons of public interest,

6.5. the transfer is necessary due to the claims held,

6.6. the transfer is necessary to protect the vital interests of the data subject or

6.7. the transfer will be made from a public register.

7. CO -ADMINISTRATION OF PERSONAL DATA

1. The Data Administrator, in the scope of personal data processed by him, allows the possibility of adopting a model of co-administration of personal data in accordance with art. 26 GDPR.

2. Co-administration of data may take place if the Data Administrator and at least one other entity jointly determine the purposes and methods of personal data processing. This means that in a given process of personal data processing, three conditions must be met simultaneously, i.e. the Data Administrator and at least one other entity must:

2.1. be administrators within the meaning of art. 4 point 7 of the GDPR,

2.2. must jointly determine the purposes of data processing,

2.3. they must jointly determine the methods (technical and organizational) of processing personal data.

3. If the conditions referred to in point 2 are met, the Data Administrator and at least one other entity become joint data controllers in the scope of a given personal data processing process.

4. In the case of adopting the data co-administration model, the data co-administrators, by way of joint arrangements, clearly define the respective scopes of their responsibility regarding the fulfillment of obligations under the GDPR.

8. AUDITS OF COMPLIANCE OF THE PROCESSING OF PERSONAL DATA

1. Audits of the compliance of personal data processing with the provisions on the protection of personal data and procedures implemented in the structure of the Data Administrator, until the appointment of the DPO, are carried out by the Data Administrator.

2. The Data Administrator performs the audit in accordance with the prepared audit plan.

2. The Data Administrator prepares an audit plan for a period not shorter than a quarter and not longer than a year, with the indication that the plan must include at least one audit.

3. In the audit plan, the Data Administrator takes into account, in particular:

3.1. the subject, scope and timing of individual audits as well as the manner and scope of their documentation,

3.2. audited personal data processing processes,

3.3. the need to verify the compliance of personal data processing with:

3.3.1. the rules for the processing of personal data, 3.3.2.

rules regarding the protection of personal data, 3.3.3.

the rules for the transfer of personal data.

4. During the audit, the Data Administrator performs and documents activities to the extent necessary to assess the compliance of personal data processing with the provisions on the protection of personal data and to prepare a report, and after its completion, prepares a report.

5. The template of the audit report is attached as Annex 8 to the Policy.

9. IMPLEMENTATION OF THE RIGHTS OF DATA SUBJECTS

1. The Data Administrator takes into account in the processes of personal data processing taking place in its structure, procedures and rules facilitating the data subject to exercise his rights under the provisions of the GDPR, including in particular:

   1.1. the right to withdraw consent (Article 7 (3) of the GDPR),

   1.2. the right of access by the data subject (Article 15 of the GDPR),

   1.3. the right to rectify data (Article 16 of the GDPR),

   1.4. the right to delete data (*the right to be forgotten*) (Article 17 of the GDPR),

   1.5. the right to limit processing (Article 18 of the GDPR),

   1.6. the right to transfer data (Article 20 of the GDPR),

   1.7. the right to object (Article 21 of the GDPR),

   1.8. the right not to be subject to decisions based on automated processing (Article 22 of the GDPR).

2. The procedure for exercising the rights of data subjects is Annex 7 to the Policy.

10. PERSONAL DATA PROTECTION BY DESIGN AND PERSONAL DATA PROTECTION BY DEFAULT

1. The Data Administrator implements appropriate technical and organizational measures designed to effectively implement the principles of data protection, provide data processing with the necessary safeguards and ensure the protection of the rights of data subjects.

2. When implementing appropriate technical and organizational measures, the Data Administrator takes into account:

2.1. state of technical knowledge,

2.2. implementation cost,

2.3. nature, scope, context and purposes of data processing,

2.4. the risk of violating the rights or freedoms of natural persons with a different probability of occurrence and the severity of the risk resulting from the processing.

3. The Data Administrator implements such technical and organizational measures that by default only personal data necessary to achieve a specific processing purpose are processed, taking into account: the amount of personal data collected, their scope, the period of their storage and their availability to other people.

4. In particular, the technical means and organizations involved must ensure that personal data is not made available to an indefinite number of persons by default.

5. First of all, the Data Administrator considers whether the purpose of the designed solution is possible to achieve without the need to process personal data. If so, choose this solution.

6. The Data Administrator ensures that the fulfillment of the conditions set out in points 1-5 (the socalled *privacy by design* and *privacy by default rules*) is properly documented, e.g. in the form of a note, e-mail, report on the IT system tests carried out, printout from the system screen.

7. A general description of the organizational security measures implemented in the Data Administrator's structure is provided in Annex 9 to the Policy.

8. A general description of the technical security measures implemented in the Data Administrator's structure is provided in Annex 10 to the Policy.

11. DATA PROTECTION IMPACT *ASSESSMENT*

1. The Data Administrator performs a data protection impact assessment to describe the processing of personal data and assess its necessity and proportionality, as well as to help manage the risk of violating the rights and freedoms of natural persons resulting from the processing of their personal data.

2. In the structure of the Data Administrator, the impact assessment for the protection of personal data is an accountability tool that facilitates compliance with the requirements set out in the GDPR,

as well as demonstrating that appropriate measures have been taken to ensure compliance with the provisions of the GDPR.

3. Data *protection impact assessment* procedure constitutes Appendix No. 6 to the Policy.

12. PERSONAL DATA PROTECTION INCIDENTS

1. The persons responsible for the security of personal data, in particular for preventing the access of unauthorized persons to the premises and systems in which personal data are processed and for taking appropriate actions in the event of detecting incidents of personal data protection, are: the Data Administrator, while in the case of appointing the DPO and ASI - also these people (with ASI in relation to data processed in IT systems).

2. The procedure for dealing with incidents of personal data protection is attached as Appendix 5 to the Policy.

13. GENERAL RULES FOR THE SECURITY OF PERSONAL DATA PROTECTION

1. Only employees authorized to process them may have access to personal data.
2. The presence of unauthorized persons in the room where personal data is processed is allowed only in the presence of a person authorized to process them, unless the data is adequately protected against access.
3. Employees with access to personal data may not disclose them both at the workplace and outside of it, in a way that goes beyond the activities related to their processing, within the scope of their official duties, as part of the granted authorization to process data.
4. Employees who store personal data are obliged to secure the materials containing data in a way that prevents access by unauthorized persons.
5. It is unacceptable to take materials containing personal data outside the area of their processing without connection with the performance of official activities. In this case, the person carrying them out and their immediate superior are responsible for the safety and return of materials containing personal data.
6. Individual passwords and identifiers for IT systems should not be shared with anyone.
7. *copy* is required to send serial e-mail messages .
8. You cannot provide information on personal data to other entities on the basis of a request for such data in the form of a telephone inquiry.
9. At the place of processing personal data recorded in paper form, employees are obliged to apply the principle of the so-called a *clean desk* , which means not leaving materials containing personal data in a place where they can be physically accessed by unauthorized persons. Each employee is responsible for the implementation of the above principle. Personal data should not be left in generally accessible places, such as desks, countertops, window sills.
10. Destruction of dirty papers, incorrect or unnecessary copies of materials containing personal data must be carried out in a way that makes it impossible to read the content, e.g. using shredders.
11. Each employee who has access to the data is individually responsible for the security of personal data processing in a specific set.

12. During the temporary absence of employees in the premises, during working hours and after the end of work, they are obliged to lock the rooms or buildings included in the areas in which personal data are processed.

13. Keys to the rooms where personal data are processed must not be left in the lock in the door. Employees are required to exercise due diligence in order to protect the keys against unauthorized disclosure.

14. Before leaving the room where personal data is stored, make sure that it has been properly secured (closed windows, doors).

15. After finishing work in the IT system in which personal data is stored, log out of the system.

16. A person using a portable computer containing personal data is obliged to exercise particular care during its transport, storage and use outside the area where personal data are processed.

17. The employee working remotely is obliged to adequately secure the data so that third parties do not have access to personal data.

18. Personal data sent electronically should be secured with a password. This password should be sent over a separate telecommunications channel.

14. REVIEWS AND UPDATES OF THE PERSONAL DATA PROTECTION POLICY

1. The policy and its attachments are periodically reviewed in terms of its adequacy, at least once a year.

2. The Policy is reviewed by the Data Administrator.

3. The review should include, in particular, an assessment of the Policy's adequacy to:

   3.1. processes operating within the Data Administrator's structures,

   3.2. applicable legal provisions relating to the protection of personal data to which the Data Administrator is subject.

4. Whenever the legal provisions that are the source of the obligations indicated in the Policy change, or there are significant factual changes within the Data Administrator's structure, the Policy review is carried out immediately.

5. If, as a result of the review of the Policy or its Annexes, it is found that it is necessary to update their provisions, the Data Administrator updates the Policy or Annexes to the extent required.

15. ATTACHMENTS

Appendix 1 List of personal data files along with the processing of personal data

Appendix No. 2 Principles of personal data retention

Appendix No. 3 The procedure for training and granting authorizations to process personal data

Appendix No. 4 Specimen of the record of persons authorized to process personal data

Appendix No. 5 Procedure for dealing with incidents of personal data protection

Appendix No. 6 Data *protection impact assessment* procedure

Appendix No. 7 Procedure for exercising the rights of data subjects

Appendix No. 8 Template of the compliance audit report on the processing of personal data

Appendix No. 9 General description of organizational security measures

Appendix No. 10 General description of technical security measures

Appendix No. 11 Specimens of appointment and dismissal of the Data Protection Officer

Annex No. 12 Patterns of appointment and dismissal of the IT Systems Administrator