DEMO

(40% of full document)

PERSONAL DATA SECURITY POLICY
AT

.....

PART ONE - DISTRIBUTION OF DUTIES

§ 1

The person engaged in an economic activity, acting as a personal data controller (hereinafter "PDC"), is responsible for the implementation of the duties described in this policy.

In the case of legal persons, an alternative wording of § 1 should be applied:

§ 1

The head of the organisational structure, acting on behalf of .....(company, entity name)....., as the Personal Data Controller (hereinafter „PDC") shall be responsible for the implementation of the duties described in this policy.

§ 2

A PDC can appoint a data protection plenipotentiary who will directly implement the tasks on behalf of the PDC, especially the tasks such as risk assessment (based on the procedure described in Appendix No.7) and examination of personal data breaches (based on the procedure described in Appendix No. 14).

§ 3

A detailed scope of the data protection plenipotentiary activities should each time be specified exhaustively in the authorisation granted to him/her, a specimen of which is included in **Appendix No. 12.**

§ 4

A PDC can appoint an IT system administrator (hereinafter "ITSA") responsible for ensuring continuous and safe IT system operation, especially granting and withdrawing authorisation on behalf of the PDC for individual applications, software, operation systems and electronic appliances, carrying out IT inventory control as specified in chapter 3 of this document and, if necessary, securing the information necessary for establishing data protection breaches related to the IT system.

§ 5

A detailed scope of the ITSA's activities should each time be specified exhaustively in the authorisation granted to him/her, a specimen of which is included in **Appendix No. 12a.**

§ 6

The PDC's failure to appoint an ITSA does not release the PDC from the obligations with regard to ensuring continuous and safe IT system operation.

§ 7

The PDC can grant access to the personal data processed solely to those who have been effectively acquainted with an abstract of the basic rules of personal data security (**Appendix No. 9**), have undertaken to comply with such rules in a statement (specimen - **Appendix No. 10**), and who received an authorisation (specimen - **Appendix No. 11**) with a precise scope of the activities involving access to personal data.

§ 8

The PDC should keep a record of the persons authorised to process personal data based on the specimen constituting **Appendix No. 11a**.

§ 9

If a Data Protection Officer is appointed, his or her scope of duties shall be specified in the document of appointment, the specimen of which is attached hereto as Appendix No. 12b. If it is stated in the document of the Data Protection Officer's appointment that his or her duties include the duties initially assigned to a data protection plenipotentiary, it is accepted that they are vested in the Data Protection Officer.

PART TWO – INVENTORY CONTROL OF INFORMATION RESOURCES

§ 1

The PDC performs and keeps an inventory of the processed information which may constitute personal data.

§ 2

Inventory control of information resources consists in determining the following in an exhaustive and comprehensive way:

a) the categories of information which are processed
b) in what way
c) for what purpose
d) on what legal basis
e) at which location
f) for how long
g) who can have access to them

§ 3

Inventory control of information resources is recorded in the form of a document, the specimen of which constitutes **Appendix No. 1**.

§ 4

The inventory control of information resources should provide a clear answer with regard to what information the entrepreneur is a PDC, and with regard to what information the entrepreneur is just a processor mandated with processing for a specific purpose by another data controller. The PDC should keep a record of all the concluded processing agreements based on the specimen constituting **Appendix No. 2**.

§ 5

Based on Appendix 1, having taken into account the choice of safeguards made as part of a risk assessment, a record of processing activities is filled in, a specimen of which constitutes **Appendix No. 3**. If acting as an entity entrusted with processing by another controller under Article 28 of the GDPR, a record of all the categories of processing activities performed for any of the controllers should be maintained in the form constituting **Appendix No. 3a**.

§ 6

Irrespective of the form of inventory control records and the form of a record of processing activities, the PDC must make a list of the buildings and premises constituting the area of personal data processing based on the specimen constituting **Appendix No. 4** (a specimen of the processing area).

PART THREE – INVENTORY CONTROL OF IT RESOURCES

§ 1

The PDC performs and keeps an inventory of the equipment used for the processing of information which may constitute personal data (inventory control of IT resources) and software.

§ 2

Inventory control of IT resources consists in determining the following in an exhaustive and comprehensive way:

a) what equipment is used for personal data processing
b) what software is used for personal data processing
c) the categories of information processed on specific and identified equipment
d) the place where it is stored
e) the persons who may have access to the equipment

§ 3

Inventory control of IT resources is recorded in the form of a document, the specimen of which constitutes **Appendix No. 6**.

PART FOUR – RISK ASSESSMENT AND SELECTION OF SAFEGUARDS

§ 1

The PDC performs a general risk assessment consisting in assigning potential threats to personal data security to the results of the inventory control from parts one and two, along with a record and substantiation of the decisions to take specific **actions with regard to information security**.

§ 2

The PDC is obliged to account for the possibility of unauthorised or accidental:

a) destruction
b) loss
c) modification
d) unauthorised disclosure
e) unauthorised access

§ 3

Risk assessment is recorded based on the procedure described in **Appendix No. 7**.

§ 4

Risk assessment is performed from the perspective of potential negative consequences for **the people whose personal data are processed** as part of the activity conducted. A detailed explanation is included in Appendix No. 7.

PART FIVE – IMPLEMENTATION OF INFORMATION OBLIGATION

§ 1

The PDC should provide every data subject whose data are processed with the information referred to in §2, unless an exemption from this obligation is stipulated by a statutory provision.

§ 2

Any information clause to be applied should be created in accordance with the guidelines contained in **Appendix No. 8.**

PART SIX – READINESS TO IMPLEMENT THE RIGHTS OF THE DATA SUBJECTS WHOSE DATA ARE PROCESSED

§ 1