Polityka Ochrony Danych Osobowych

w Powiślańskiej Szkole Wyższej

Kwidzyn, 2018, document update: September 2023.

Table of contents

§ 1

INTRODUCTION

The Personal Data Protection Policy is a document describing the data protection principles applied by the Administrator to meet the requirements of the EP and RE Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data (RODO).

The policy is one of the organizational measures to demonstrate that the processing of personal data is carried out in accordance with the above Regulation.

DEFINITIONS:

Administrator (of the data) - The Administrator of the Personal Data is the Powisle School of Higher Education, headquartered at 11 Listopada 29 Street, 82 - 500 Kwidzyn. The Administrator is represented by Rector Dr. Katarzyna Strzała-Osuch, Prof. PSW.

The personal data controller, bearing in mind the importance of security principles in the processing of personal data, guided by the principle of protecting the fundamental rights and freedoms of individuals, and in particular their right to adequate protection of personal data, and in order to ensure the compliance of the procedures for the processing of such data with the requirements of the law, and with a view to protecting the good name of the entity, hereby establishes the Personal Data Protection Policy, i.e. the principles and safeguards applied in the processing of personal data at the University.

With the above in mind, the Administrator undertakes to comply with the basic principles relating to the processing of personal data and to demonstrate compliance with them (the principle of accountability) - which include:

a. The principle of processing personal data in accordance with the law in a fair and transparent manner.
b. The principle of limited purpose which means that personal data may be collected for specific, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
c. The principle of minimalism, which means that personal data can be processed only to the extent necessary and only for the purposes for which they are processed.
d. The principle of accuracy, according to which the data processed by the Administrator should be up-to-date and correct, while personal data that are inaccurate should be immediately deleted or corrected.
e. The principle of limited processing, which means that personal data should be kept in a form that allows identification of the data subject and for no longer than necessary for the purposes for which the data are processed.

f. The principle of integrity and confidentiality, which require that personal data be processed in a manner that ensures their adequate security, including adequate protection against unauthorized or unlawful processing and their accidental loss, destruction or damage by means of appropriate technical or organizational measures.

Anonymization- irreversible change of personal data as a result of which the data loses its character of personal data by depriving it of its identifying characteristics. Based on the anomized data, it is not possible to identify the individuals to whom the personal data originally pertained.

Personal data - means any information about an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by an identifier such as a name, identification number, IP addresses, cookie IDs, location data, Internet identifier or one or more specific factors that determine the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

Information security incident-is an accidental or unlawful event leading to the destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data.

Data Protection Officer (DPO) - is a person formally appointed by the Controller to inform and advise the Controller of the processor's compliance with applicable data protection laws and this Policy and to monitor compliance with them, and to act as a point of contact for processors and the supervisory authority.

Personal data breach - an incident of security breach of personal data leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed associated with the risk of violation of the rights or freedoms of data subjects.

Data Protection Impact Assessment - is a process carried out by the Controller, if required by applicable law and, if necessary, with the participation of the Data Protection Officer, prior to processing, where there is a likelihood of high risk to the rights and freedoms of individuals as a type of personal data processing and occurs with the use of new technologies, taking into account the nature, scope, context and purposes of the processing. This process must assess the impact of the planned processing operations on the protection of personal data.

Processing of personal data - means any activity performed on personal data in an automated or non-automated manner, e.g.:

- collection,

- consolidation,
- organizing,
- organizing,
- storage,
- adapting or modifying data,
- downloading,
- reviewing,
- exploitation,
- disclosure by message,
- dissemination or other sharing,
- matching,
- linking,
- limiting,
- deletion or destruction of data.

Processor-an entity that processes personal data on behalf of the Administrator under an entrustment agreement. The entrustment agreement should specify, among other things: the subject, purpose, time and scope of processing, as well as the type of data processed.

Pseudonymization - means the processing of personal data in such a way (e.g., by replacing names with numbers) that the personal data can no longer be attributed to a specific data subject without the use of additional information (e.g., a Reference List of Names and Numbers), provided that such additional information is stored separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

RODO - Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU L of 2016, No. 119, p.1.

Special categories of personal data - personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and include the processing of genetic data, biometric data to uniquely identify an individual, health data, data on a person's natural sex life or sexual orientation. Depending on the applicable law, special categories of personal data may also include information about social security measures or administrative and criminal proceedings and sanctions.

Profiling - is any form of automated processing of personal data that involves the use of personal data to evaluate certain personal factors of an individual, in particular to analyze or forecast aspects of that individual's performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movement.

Consent to the processing of personal data - means a voluntary, freely specified, specific, informed and unambiguous indication of the data subject, by means of a statement or a clear affirmative action, consenting to the processing of personal data related to him. It is incumbent on the Administrator to adequately document the fact of granting consent for evidentiary purposes.

§ 2

IMPACT ASSESSMENT (RISK ANALYSIS)

1. Description of processing operations (asset inventory)

In order to perform a risk analysis, it is required to identify the personal data to be secured. These data in the form of sets (categories of persons) are shown in Appendix 01a List of Personal Data Sets.

The description of the collections (categories of people) should include such information as:

a) The name of the collection (description of the category of people),
b) description of processing purposes,
c) The nature, scope, context of personal data,
d) data recipients,
e) functional description of processing operations,
f) Assets used to process personal data (Information, Programs, Operating Systems, IT Infrastructure, Infrastructure, Employees and Associates,
g) Outsourcing) - Appendix 02b List of potential assets,
h) Information about the need to enter in the register of processing activities,
i) Information on the need to conduct a harvest impact assessment.

2. Assessment of necessity and proportionality (compliance with the provisions of the RODO)

As part of conducting a risk analysis of the processing of personal data, the Administrator is required to fulfill legal obligations to data subjects.

In particular, the Administrator shall ensure that:

a) These data are legally processed,
b) the data are adequate in relation to the purposes of processing,
c) The data are processed for a specified period of time (data retention),

d) the so-called "information obligation" has been exercised with respect to these persons, along with an indication of their rights (e.g., the right of access to data, portability, rectification, deletion, restriction of processing, objection, revocation of consent),

e) consents to the processing of personal data and information clauses for the above persons have been developed (see Appendix: 01c - consents to the processing of personal data and 01b Information clauses),

f) there are entrustment agreements with processors in accordance with Annex 01g Entrustment Agreement (the list of processors is maintained in Annex 01f Register of Entrustment Agreements).

3. Risk Analysis

The procedure describes how to conduct a risk analysis to secure personal data adequately to the identified risks arising from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data.

It is assumed that the risk analysis is carried out for a set or group of sets (categories of people) or for processing processes (e.g., for a set of employees, a set of students, for the process of sending newsletter information to enrolled recipients).

3.1. Definitions

1. Assets - tangible and intangible assets that affect the processing of personal data.
2. Threat - a potential breach (potential incident).
3. Effects - the results of an unwanted incident (losses in the event of a hazard).
4. Risk - the probability that a specific hazard will occur and cause loss or destruction of resources.

3.2 Determination of risks

1. The controller is responsible for determining the list of risks that may occur in the processing of data in the collection, for categories of persons or in the processing.
2. Risks should be identified in relation to previously identified assets.
3. List of sample hazards (see Appendix 02c List of potential hazards).

3.3 Risk calculation for hazards

1. The administrator determines the Probability (P) of occurrence of particular risks in the collection or processing.
2. The proposed probability scale is presented in Table A.

3. The Administrator determines the Consequences (S) of the occurrence of incidents (materialization of threats), taking into account financial losses, loss of reputation, sanctions/criminal consequences.
4. The proposed Impact Scale is presented in Table B.
5. The administrator calculates Risks (R) for all risks and their effects w/ the formula: R = P * S.

Table A - PROBABILITY.	**LEVEL**
Very high	5
High	4
Medium	3
Low	2
Very low	1

Table B Effect	**Level**	**Description**
Very high	5	There may be irretrievable loss of data, the work of the enterprise is stopped until proper functioning is restored, large financial losses
High	4	The work of the enterprise may be stopped until the cause is removed, financial losses,
Medium	3	Work of the company is disrupted, should restore the proper state of security
Low	2	The operation of the enterprise is running smoothly, small-scale financial losses may occur
Very low	1	No impact on the operation of the company

3.4 Comparison of calculated risks with the scale and determination of further handling of risks

1. The administrator compares the calculated risks with the scale and makes decisions on how to further deal with the risks.
2. The proposed Risk scale is presented in Table C.

Table C - Risk Matrix			IMPACT				
			B. low	Low	Medium	High	B. high
			1	2	3	4	5
	B. high	5	Ś	W	K	K	K

Probability	High	4	Ś	W	W	K	K
	Medium	3	N	Ś	W	W	K
	Low	2	N	N	Ś	W	W
	B. low	1	N	N	Ś	W	W

Risk level:

N - from 1 to 4 - low, the level of risk is acceptable, action should be taken on the basis of the effort needed to reduce it

¶ - up to 5 to 7 - medium, risk level unacceptable, however, action can be taken at a later date subject to periodic inspection

W - from 8 to 15 - high, risk level unacceptable, action can be taken at a later date, while constantly monitoring the situation

K - from 16 to 25 - critical, unacceptable level, requires immediate action.

3.5 Response to the value of risk

1. Risk acceptance - safeguards are adequate - no need for additional safeguards.
2. Risk-reducing actions that the Administrator can apply:
   1) Transfer -transfer of risk (outsourcing, insurance),
   2) Avoidance - eliminating activities that cause risk (e.g., banning laptops from being taken outside the organization),
   3) Reduction - the use of security features to reduce risk (e.g., encrypting data pendrives taken outside the company).
3. List of sample safeguards (see Appendix 02d List of potential safeguards).
4. The risk analysis is carried out in a special template (program), (Appendix 02e RODO Risk Analysis Sheet).

3.6 Re-analyzing the risks

Re-analysis of risks is carried out periodically or after significant changes in data processing (e.g., processing of new collections, new processing processes, legal changes).

4. Risk management plan

1. Wherever the Administrator decides to reduce the risk, he sets a list of safeguards to be implemented, the deadline for implementation and the people responsible
2. The administrator is required to monitor the implementation of security features.

§ 3

AUTHORIZATIONS

1. The Administrator is responsible for granting and cancelling authorizations to process personal data collected in paper files and information systems.
2. The Administrator may delegate the above authority to the Data Protection Officer.
3. The employee affairs department is obliged to provide the Administrator and the Data Protection Officer with information about a newly hired employee or the establishment of cooperation on the basis of a civil law contract in connection with the performance of which it is advisable and necessary to grant the employee/contractor authorization to process data in paper files and computer systems. The employee affairs department is obliged to indicate the collection of personal data and the scope of authorization, which is purposeful and necessary for the performance of official or contracted activities.
4. The employee affairs department is obliged to immediately notify the Administrator and the Data Protection Officer of the fact of termination of the employment contract, termination of the employment contract or termination of the cooperation agreement, as well as any other event (e.g., change in the scope of duties) - due to which it is necessary to cancel or change the scope of authorization to process personal data for a particular employee or contractor.
5. The processing of personal data by an employee or contractor may be carried out only on the basis and within the scope of the law, including on the basis of a written authorization for the processing of personal data or a business order issued and confirmed by the Administrator or the Personal Data Inspector.
6. Authorizations specify the scope of operations on data, e.g., creation, deletion, inspection, transfer (Appendix 01e Authorization to process personal data).
7. Authorizations can be given in the form of orders, such as authorization to conduct inspections, audits, perform official activities, a documented order from the administrator in the form of an entrustment agreement.
8. The Data Protection Officer shall maintain records of authorized persons in order to control the proper access to data of authorized persons (Annex 01d Records of authorized persons).

§ 4

INSTRUCTIONS FOR DEALING WITH VIOLATIONS / INCIDENTS

The procedure defines a catalog of vulnerabilities and breaches/incidents that threaten the security of personal data and describes how to respond to them. Its purpose is to minimize the impact of security breaches/incidents and reduce the risk of threats and the occurrence of breaches/incidents in the future.

1. Each person authorized to process personal data is required to notify his/her immediate supervisor or the Data Protection Officer when a vulnerability is identified or a breach/incident occurs.
2. Typical personal data security vulnerabilities include:
   a) inadequate physical security of premises, equipment and documents,
   b) Inadequate security of IT equipment, software against leakage, theft and loss of personal data,
   c) Failure of employees to comply with data protection rules (e.g., failure to apply the clean desk/screen rule, password protection, failure to lock rooms, cabinets, desks).
3. Typical personal data security incidents include:
   a) external random events (fire of the facility/room, flooding with water, loss of power, loss of communications),
   b) internal random events (failures of the server, computers, hard disks, software, mistakes of IT specialists, users, loss / misplacement of data),
   c) Intentional incidents (hacking of the IT system or premises, theft of data/equipment, leakage of information, disclosure of data to unauthorized persons, deliberate destruction of documents/data, viruses and other malware).
4. If an incident is identified, the Administrator (or, if appointed, the IOD) conducts an investigation during which:
   a) Determines the scope and causes of the incident and its possible consequences,
   b) initiates possible disciplinary action,
   c) Works to restore the organization's operations after an incident,
   d) recommends preventive (precautionary) measures to eliminate similar incidents in the future or reduce losses when they occur.
5. The Administrator shall document the above all breaches of personal data protection, including the circumstances of the breach of personal data protection, the consequences of the breach and the remedial actions taken - (Annex 03 Records of breaches/incidents).
6. It is forbidden to knowingly or unintentionally cause incidents by persons authorized to process data.
7. In the event of a breach of personal data protection resulting in a risk of violation of the rights or freedoms of individuals, the controller shall without undue delay - as far as possible,

no later than 72 hours after the discovery of the violation - shall report it to the supervisory authority.

§ 5

DATA PROTECTION REGULATIONS

1. The Regulations are intended to provide knowledge to those processing personal data regarding secure processing rules. It can be found in the appendix - 04 Regulations for the Protection of Personal Data.
2. After becoming familiar with the data protection rules, individuals are required to confirm their knowledge of these rules and declare their application, can be found in Appendix 04a Employee confidentiality statement/ for those carrying out other assignments.

§ 6

TRAINING

1. Each person should be trained and familiarized with the provisions of RODO before being allowed to work with personal data.
2. The Personal Data Inspector is responsible for conducting the training.
3. If an internal training course on data protection principles is conducted, it is advisable to document the training with Appendix 05a RODO Training Plan.
4. Training materials for trainees were developed in the form of Appendix 05b RODO Internal Training.
5. After training on data protection principles, participants are required to confirm their knowledge of these principles and declare their application, see Appendix 04a Confidentiality Statement.

§ 7

REGISTER OF PROCESSING OPERATIONS

1. If it is necessary for the Administrator to maintain a register of processing activities, it shall complete Appendix 06a Register of Activities Maintained by the Administrator.
2. If it is necessary for the Processor to keep a register of processing activities, the Processor shall complete Appendix 06b Register of Activities Maintained by the Processor.

§ 8

AUDITS

1. According to Article 32 of the RODO, the Administrator should regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing.
2. For this purpose, the Administrator uses the audit procedure - (Appendix 07 Audit Procedure).

§ 9

PROCEDURE FOR RESTORING AVAILABILITY OF AND ACCESS TO PERSONAL DATA IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT (BCP)

According to Article 32 of the RODO, the Administrator should ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident. The Administrator has developed restoration procedures as described in Annex 08 Business Continuity Plan.

§ 10

LIST OF SECURITY FEATURES

1. The Administrator shall maintain a list of safeguards it applies to protect personal data, described in the appendix Information Systems Management Manual/RODO Security List.
2. The instruction/list indicates the procedural safeguards used and the safeguards as technical and organizational measures.
3. The manual / list is updated after each risk analysis / impact assessment.

Dr. Katarzyna Strzała-Osuch, Prof. PSW

Rector