PERSONAL DATA PROTECTION AFTER IMPLEMENTATION OF NEW „GDPR (RODO)” REGULATIONS

INTERNAL TRAINING

Legal basis:

1. GENERAL DATA PROTECTION REGULATION (GDPR/RODO) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – defines provisions on the protection of personal data

2. The Law of 10 May 2018 on personal data protection (Journal of Laws, item 1000)

Objectives and substance of GDPR:

- Legal act in force in all European Union Member States
- More effective protection of data in the age of technical development and globalisation
- Harmonising the regulations in all Member States of EU and ensuring free flow of personal data among these countries

ABI = DSA

(Administrator Bezpieczeństwa Informacji = Data Security Administrator)

↓

IOD = DPO

(Inspektor Ochrony Danych = Data Protection Officer)

GIODO

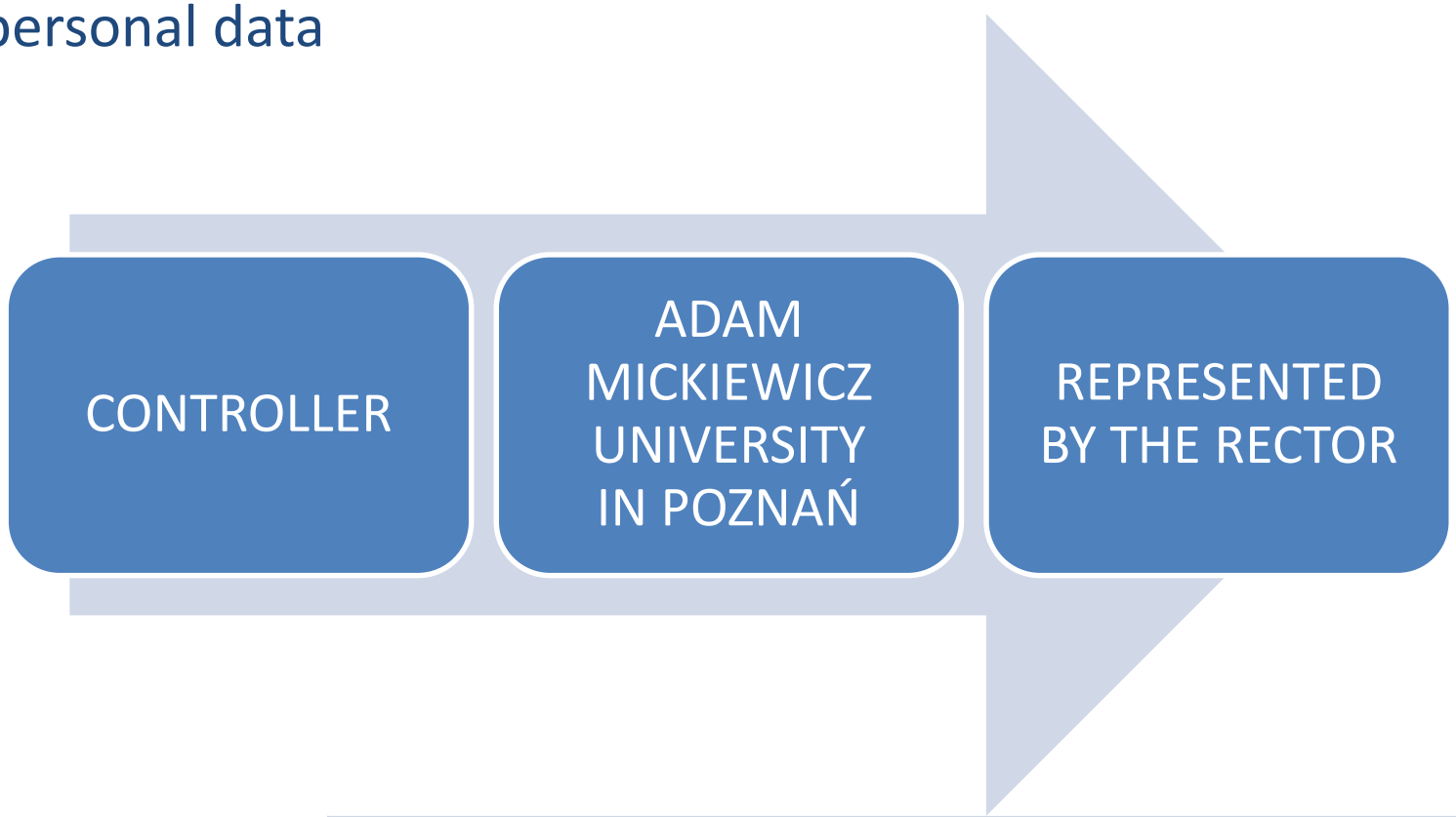
(Główny Inspektor Ochrony Danych Osobowych = Inspector General for the Protection of Personal Data)

↓

UODO

(Urząd Ochrony Danych Osobowych = Office for the Protection of Personal Data)

CONTROLLER (art.4.7 GDPR) – natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data



DATA PROTECTION OFFICER art.37,38,39 GDPR – informs and advises the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation; monitors compliance with this Regulation; acts as the contact point for the supervisory authority on issues relating to processing, including the prior consultation where appropriate.

ELECTRONIC COMMUNICATION SYSTEM OFFICER – appointed by the controller to ensure the proper functioning of electronic communication systems.

DATA SUBJECT – natural person, whose personal data are processed

PROCESSOR (art. 4.8 GDPR) – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

PERSONAL DATA (art. 4.1 GDPR) – any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person:

- Name, correspondence address/phone
- Name, number of the person's identification document
- Name, bank account number
- Social security number (Pesel)
- Location data
- Monitoring, phone records
- E-mails

SPECIAL CATEGORIES OF PERSONAL DATA (art. 9 GDPR) – include:

- Physical or mental health of a natural person e.g. medical records, disability, dislexia, Company Social Benefits Fund information
- Genetic data, e.g. DNA, biological samples
- Biometric data such as facial images, dactyloscopic data, voice
- Data relating to criminal convictions and offences, e.g. criminal record
- Racial or ethnic origin
- Political opinion, religion or beliefs
- Trade union membership
- Sexual orientation

DATA PROCESSING (art. 4.2 GDPR) - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:

- collection
- recording
- organisation
- structuring
- storage
- adaptation
- alteration
- retrieval
- consultation
- use
- disclosure by transmission
- dissemination or otherwise making available
- alignment
- combination
- restriction
- erasure
- destruction

DATASET – structured set of data available according to specific criteria

Paper form	• personnel files • folders • documents
Electronic form	• programs, computer system • files • folders
Recorder recordings	• surveillance footage • phone recording

Main rules (art.5.1 RODO)

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY
2. PURPOSE LIMITATION
3. DATA MINIMISATION
4. ACCURACY
5. STORAGE LIMITATION
6. INTEGRITY AND CONFIDENTIALITY
7. ACCOUNTABILITY

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY (art.5.1a GDPR)

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For this purpose the Controller is obliged to:

- Ensure the lawfulness of data processing *(art. 6, 9)*
- Provide the information where personal data are collected *(art. 13, 14)*
- Record processing activities *(art. 30)*

LAWFULNESS OF PROCESSING (art. 6 GDPR):

- the data subject has given consent to the processing of his or her personal data

CONSENT OF A PERSON (art. 4.11 GDPR) – freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (e.g. ticking a box when visiting an Internet website).

The data subject shall have the right to withdraw his or her consent at any time. It shall be as easy to withdraw as to give consent.

- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; *(PERFORMANCE: civil-law contract, lecture, employment contract, delivery)*
- processing is necessary for compliance with a legal obligation to which the controller is subject *(Labour Code, Law on Higher Education, Archives Law)*

- processing is necessary in order to protect the vital interests of the data subject or of another natural person; (*natural disasters, notifying a person in a crisis situation)*
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller *(activities of foundations, associations, associations in the work places, health institutions, social protection, healthcare, the 500+ regulation)*
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject *(direct marketing, recovery, correspondence register, register of entries, monitoring, customer service, co-workers)*

2. PURPOSE LIMITATION – the rule of compatibility and purpose (art. 5.1b GDPR)

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Further processing is possible ONLY for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3. DATA MINIMISATION (art. 5.1c GDPR)

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

ONLY these personal data shall be collected, which are absolutely necessary for the purpose execution for which they are collected and processed (minimal amount of data).

4. ACCURACY (art. 5.1d GDPR)

Personal data must be accurate and kept up to date.

Every reasonable step must be taken to ensure that personal data that are inaccurate will be immediately erased or rectified without delay.

5. STORAGE LIMITATION (art. 5.1e GDPR)

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6. INTEGRITY AND CONFIDENTIALITY (art. 5.1f GDPR)

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

PERSONAL DATA PROCESSING REQUIRES MANDATES

(art. 29 GDPR)

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

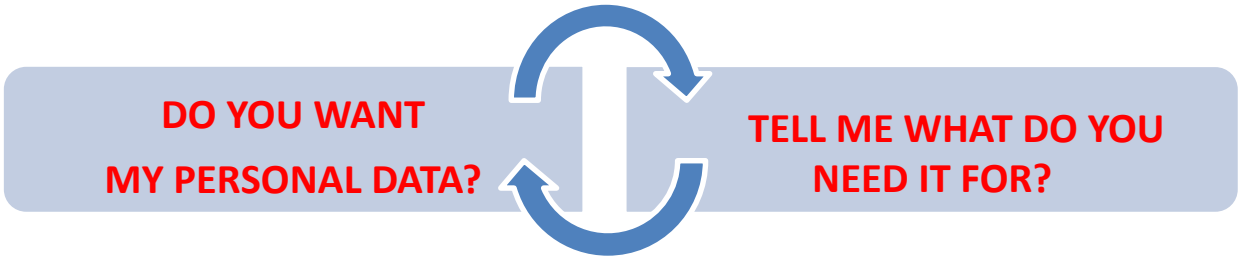
The Controller issues relevant **MANDATES TO PROCESS PERSONAL DATA** (stored in personal files) following a training from the scope of personal data protection and making a declaration of data confidentiality.

PROCESSING PERSONAL DATA WITHOUT HAVING MANDATE TO PROCESS IT IS AGAINST THE LAW!

7. ACCOUNTABILITY (art. 5.2 GDPR)

The controller is responsible for, and must be able to demonstrate, compliance with personal data protection regulations and prove the implementation of internal mechanisms and procedures.

OBLIGATION TO PROVIDE INFORMATION (art. 13 GDPR)



Where personal data relating to a data subject are collected from the data subject, the controller shall provide the data subject with all of the following information:

- the identity and the contact details of the controller or controller's representative
- the contact details of the Data Protection Officer
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the recipients or categories of recipients of the personal data
- the fact that the Controller intends to transfer personal data to a third country or international organisation

- the period for which the personal data will be stored
- the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- the right to withdraw consent at any time
- the right to lodge a complaint with a supervisory authority (UODO)
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and of the possible consequences of failure to provide such data
- whether personal data will be subject to profiling, and what will be the consequences of such processing for the data subject

RIGHT TO ERASURE „RIGHT TO BE FORGOTTEN" (art. 17 GDPR)

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- Data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing
- Data subject objects to the processing
- Personal data have been unlawfully processed
- Personal data have to be erased for compliance with a legal obligation
- Personal data have been collected in relation to the offer of information society services

RIGHT TO DATA PORTABILITY (art. 20 GDPR)

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

The processing is based on consent or on a contract and the processing is carried out by automated means (transfer of personal data from one bank to another, from one network to another).

PROFILING (art. 22 GDPR) – any form of automated processing of personal data aiming at assessing, analysing and forecasting the material situation, health status, preferences, location of the person and results in legal consequences against that person or in any other way affects this person.

The data subject has the right not to give his or her consent for profiling the personal data.

Examples of profiling:

- Automatic credit risk assessment or insurance premium
- Tracking location through mobile applications, loyalty programmes
- Behavioural advertisements
- Tracking, tracing, content on the Internet

According to art. 33 GDPR, **ANY incidents affecting human rights and freedom must be reported to UODO (Urząd Ochrony Danych Osobowych) within 72 hours** *(falsifying of data, loss of control of personal data)*

The data subject should be informed, if the infringement of his or her rights can cause serious risk.

The Controller is obliged to carry out the recording of such incidents.

Detailed instructions of reporting infringement of personal data protection at Adam Mickiewicz University is provided at the AMU website
www.odo.amu.edu.pl

The knowledge base from the scope of personal data protection, current provisions and legislation, trainings, internal documents and regulations concerning the rules of personal data protection are also provided.

According to art. 35 GDPR, in order to implement adequate protection means to properly process personal data, the Controller shall carry out a data protection impact assessment of personal data.

The data protection impact assessment includes:

1. Identification, description and evaluation of processing operations (*categories subject to processing, purposes, transfer-acceptance protocols, assets subject to processing)*
2. Assessment of the compliance with GDPR (RODO) provisions

3. Risk assessment:
    - Setting out the risks
    - Quantifying the risks – likelihood of occurrence of particular risks
    - Cross-referencing of the quantified risks with the scale
    - Planning reaction for the risk value
    - Re-examination

4. Plan, how to handle the risk

In order to minimise the risk and avoid the data breach the Controller implements the following technical and organisational measures:

1. Organisational security
2. Physical security
3. Technical security
4. IT security
5. External security

ORGANISATIONAL SECURITY

- **PROCEDURES** – Security Policy, Personal Data Protection Regulations, Administering the Mandates
- **TRAININGS**
- **AUDITS**

PHYSICAL SECURITY

Ensuring the protection of premises, infrastructure and equipment by:

- Key policy
- Physical access control – key cards, biometric system, reception
- Clean desk policy

TECHNICAL SECURITY

- Fire protection system – smoke detectors, fire suppression systems
- Environmental monitoring – humidity sensors, temperature sensors
- Air conditioning in the server room
- Video surveillance
- UPS system / power generators

IT SECURITY – ensure the protection of personal data processed in the IT systems:

- Anti-virus and anti-spam softwares, filtering instruments
- Data encryption
- Backup files
- Password policy
- Clear screen policy (screen savers with passwords, screen settings)
- Interdiction of copying and installing unauthorised software from the Internet
- Interdiction of using auto completion option and password memorization

IT SECURITY

- ONLY the **university e-mail address** can be used for the work-related purposes
- Serial correspondence can be sent ONLY as **BCC**
- Suspicious attachments and links should not be opened/loaded
- Working within unlocked Wi-Fi should be avoided
- Laptops should be transported in the trunk
- One should **log out** from all the used systems after the ended work
- Every user should use only his or her own account (identifier)

EXTERNAL SECURITY

Access procedures for third-party bodies:

- confidentiality clause/arrangements drawn up for the external bodies having access to personal data at the premises of the organisation

- entrustment agreement of personal data processing signed by the parties, which process personal data externally in the form of „outsourcing”

ADMINISTRATIVE FINES (art.83 GDPR)

FINES up to 10 mln. EUR, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, for non-compliance with the law in regard to personal data processing

FINES up to 20 mln. EUR, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, for non-compliance with the law in regard to processing of special categories of personal data

FINES up to 100 000 PLN, in the case of a public body, for non-compliance with the law in regard to personal data processing

FINES up to 200 000 PLN, in the case of a public body, for non-compliance with the law in regard to processing of special categories of personal data

NOTE!

According to art. 82.1 GDPR, „any person who has suffered material or non-material damage as a result of an infringement of this Regulation **shall have the right to receive compensation from the controller or processor for the damage suffered.**”