



**INFORMATION SECURITY,
INCLUDING PERSONAL DATA
PROTECTION –
BASIC CONCEPTS AND
INFORMATION**

INFORMATION SECURITY REGULATIONS

1. Generally applicable provisions of law:

- directives
- regulation
- Constitution
- Act

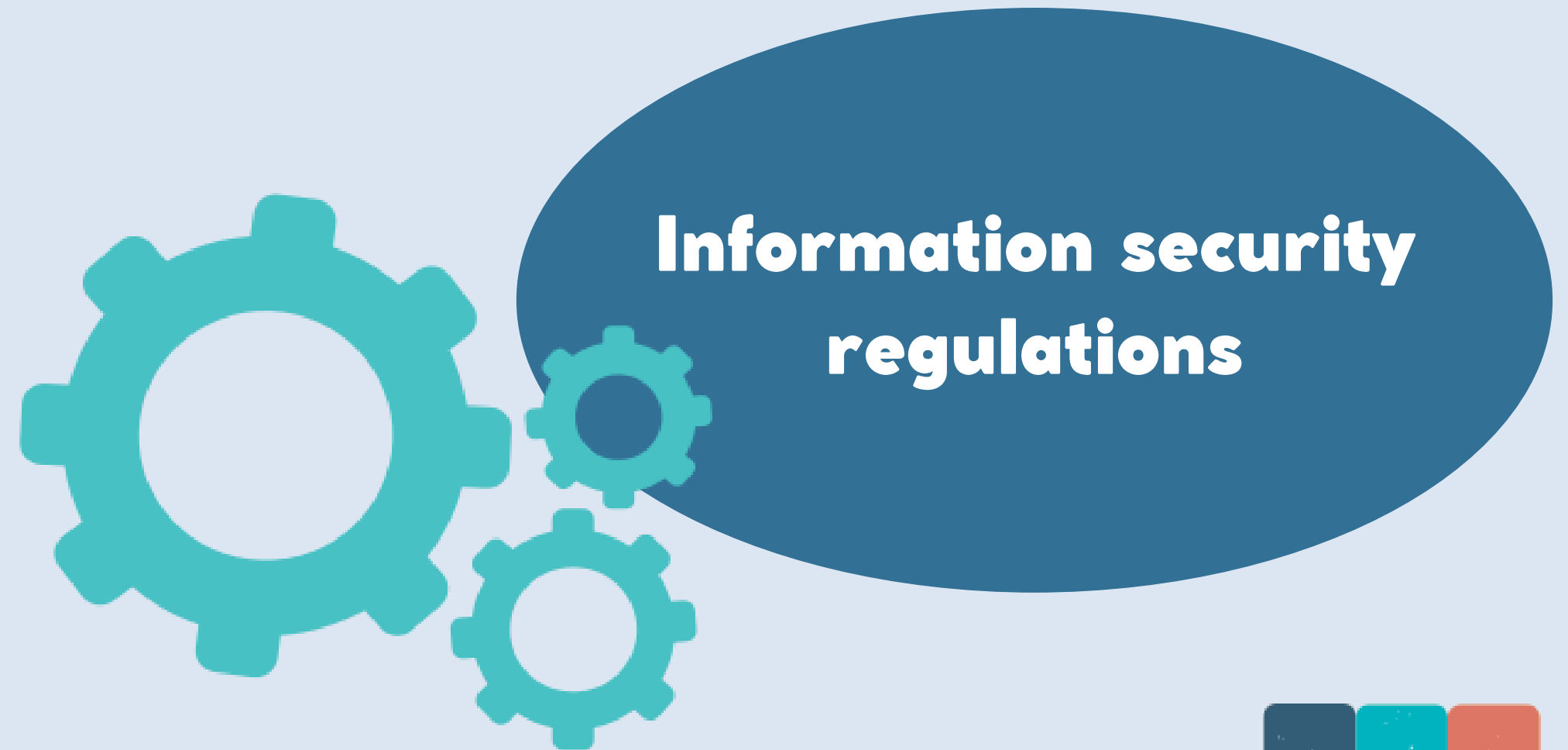
2. Polish standards

3. Administrative decisions

4. Codes of conduct

5. Guidelines, guides

List: Annex No. 11 to the Quality Manual - LIST OF DOCUMENTS RELATED TO QB
- Dz-21.0 "INFORMATION SECURITY POLICY".



INFORMATION SECURITY REGULATIONS

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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) (the so-called General Data Protection Regulation personal data, abbreviated as GDPR) (date of application: May 25, 2018).

The Act of 10 May 2018 on the Protection of Personal Data

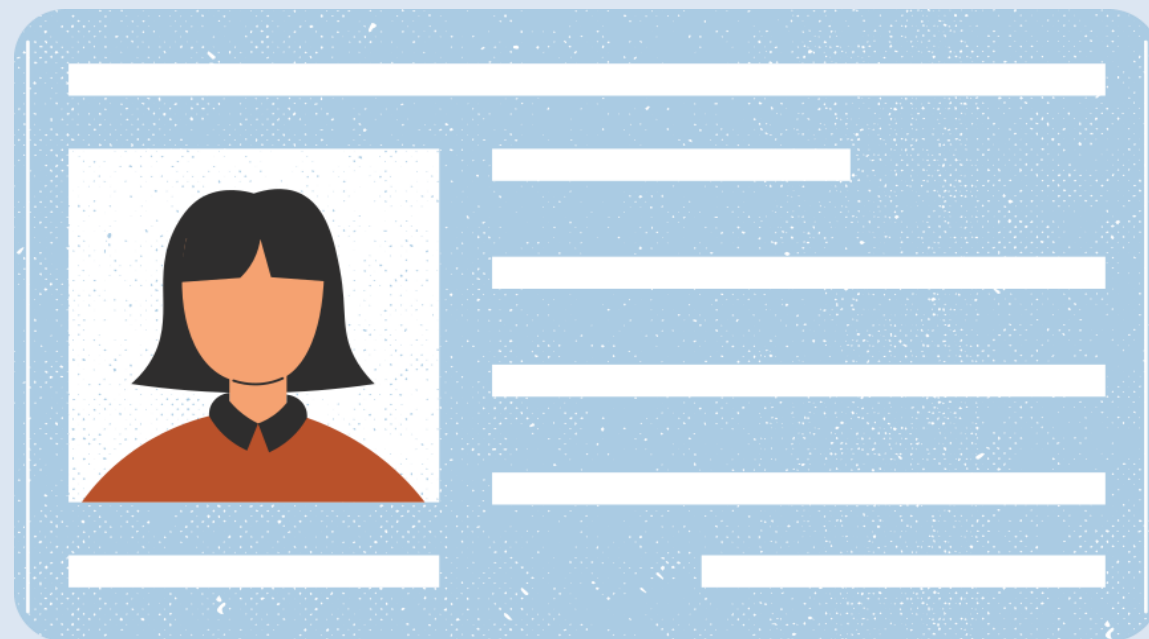


The previously applicable Act of 29 August 1997 on the protection of personal data has been repealed.



PERSONAL DATA

Personal data – 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 reference to an identifier such as:

- first name and last name,
- ID number,
- location data,
- online ID or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

Personal data is information in the form of messages (regardless of the way they are recorded), e.g. in the form:

- words,
- sounds,
- photography.

PERSONAL DATA -CONT.



Examples of identified or identifiable persons:

- Head of the UCK Medical Equipment Department
- Data Protection Officer
- Monika, Chief of Information Security Management System UCK
- jkraszewski@uck.gda.pl
- Head of Emergency Room UCK (KOR)
- UCK Chief Executive Officer
- Aleksandra D., President of the City of Gdańsk
- vocalist of the band "Hey,,
- writer, author of the Fjällbaka saga
- CEO of Tesla Inc.
- movie director, winner of the Academy Award (Oscars) for 2021
- Anna L., personal trainer, wife of a well-known Polish footballer.

You possibly know the identity of these people or can easily verify.

HEALTH RELATED DATA

HEALTH RELATED DATA

- personal data about an individual's physical health,
- personal data about an individual's mental health, including data on the use of healthcare services - revealing information about the individual's state of health.

EXAMPLES

- information collected during a patient registration for healthcare services or when healthcare services are being provided,
- a mark attributed to a natural person to uniquely identify that natural person for health purposes (e.g. a general ledger number),
- information derived from laboratory or medical examinations,
- any information on past or current medical conditions.



"ORDINARY" PERSONAL DATA (ART. 6 GDPR)

Art.6 par. 1 GDPR: Processing of so-called „ordinary” personal data shall be lawful only if and to the extent that at least one of the following applies:

- the data subject **has given consent** to the processing of his or her personal data (...),
- 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,
- processing is **necessary for compliance** with a legal obligation to which the controller is subject,
- processing is **necessary in order to protect the vital interests** of the data subject or of another natural person,
- 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,
- 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 which require protection of personal data, in particular where the data subject is a child.

SPECIAL CATEGORY PERSONAL DATA (ART. 9 OF THE GDPR)

Art. 9 par. 2 GDPR:

Art.9 par. 1 GDPR [stating the prohibition of processing special category of personal data] does not apply if:

- the data subject **has given explicit consent** (...), except where Union or Member State law provide that (...) may not be lifted by the data subject (...),
- processing is **necessary for the purposes of carrying out the obligations and exercising specific rights** (...) in the field of employment and social security and social protection law (...),
- processing is **necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent,
- processing is **carried out in the course of its legitimate activities with appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes (...),
- processing relates to personal data which **are manifestly made public by the data subject**,
- processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity,
- processing is **necessary for reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject,

SPECIAL CATEGORY PERSONAL DATA (ART. 9 OF THE GDPR) CONT.

Art. 9 par. 2 GDPR:



Art. 9 par. 1 GDPR [stating the prohibition of processing special category of personal data] does not apply if:

- processing is **necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 GDPR,
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy,
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (...).



PROCESSING OF PERSONAL DATA (ARTICLE 4, POINT 2, GDPR)

Processing – means 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:



Processing	Collection	Recording	Organisation
Structuring	Storage	Adaptation or alteration	Retrieval
Consultation	Use	Disclosure by transmission	Disclosure by dissemination or otherwise making available
Alignment or combination	Restriction	Erasure	Destruction

PERSONAL DATA PROCESSING ACTIVITIES. RPA AND RCPA.



Personal data processing activity - a set of interrelated operations on data, performed by one or several persons, which can be defined collectively, in connection with the purpose for which these activities are undertaken.

Register of Processing Activities (RPA) - a list of personal data processing activities maintained by the Data Administrator.

Register of Categories of Processing Activities (RCPA) – a list of categories of processing activities maintained by the Processor.

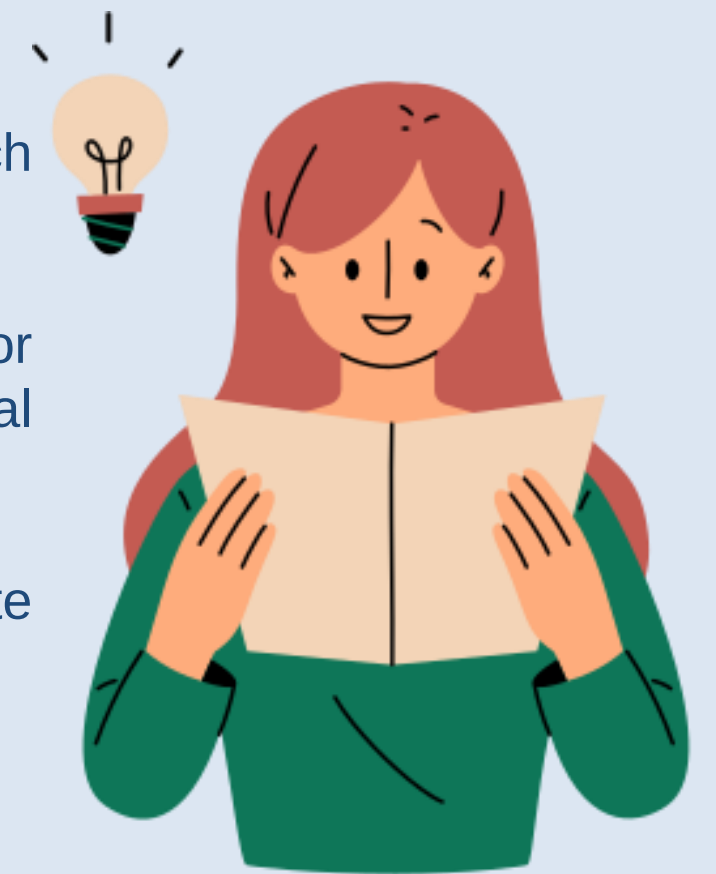


PRINCIPLES OF PERSONAL DATA PROCESSING (ARTICLE 5 OF THE GDPR)

Personal data should be:

- processed lawfully, fairly and in a transparent manner for the data subject ("**lawfulness, reliability and transparency**"),
- collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (...) ("**purpose limitation**"),
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimization**"),
- correct and, if necessary, updated (...) ("**correctness**"),
- stored in a form that permits identification of the data subject for no longer than necessary for the purposes for which the data are processed ("**storage limitation**"),
- processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("**integrity and confidentiality**"),

The administrator is responsible for compliance with the above. regulations and must be able to demonstrate compliance with them ("**accountability**").



LAWFULNESS OF THE DATA PROCESSING. BASIS FOR PROCESSING PERSONAL DATA

When is the processing of data allowed?

1

Art. 6 GDPR

Applies to 'ordinary' personal data.

2

Art. 9 GDPR

Applies to special category of personal data.

3

Art. 10 GDPR

Concerns data relating to convictions and prohibited acts.



PDA'S INFORMATION OBLIGATION (ARTICLES 13 AND 14 OF THE GDPR)

ART. 13 GDPR: If the personal data of a data subject are collected from that person, the controller shall provide the data subject with all of the following information when obtaining the personal data:

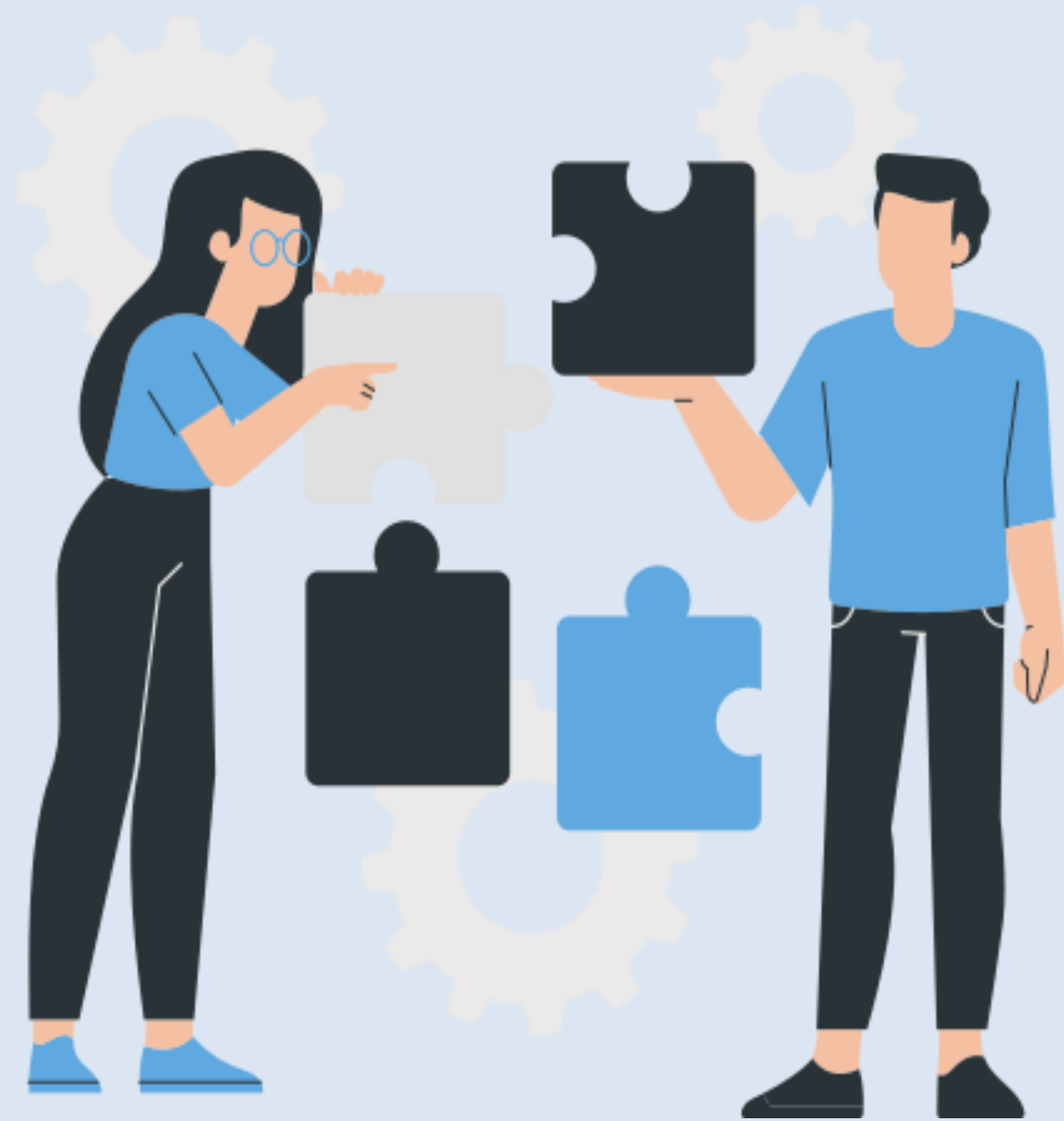
- your identity and contact details and, where applicable, the identity and contact details of your representative,
- where applicable, contact details of the data protection officer,
- the purposes of personal data processing and the legal basis for processing,
- if processing takes place pursuant to Art. 6(1) 1 letter f) – legitimate interests pursued by the administrator or a third party,
- information about the recipients of personal data or categories of recipients, if any;
- where applicable, information on the intention to transfer personal data to a third country or international organization (...)

In addition to the information referred to in section 1, when obtaining personal data, the controller provides the data subject with the following other information necessary to ensure reliability and transparency of processing:

- the period for which personal data will be stored, and if this is not possible, the criteria for determining this period,
- information about the right to request from the administrator access to personal data relating to the data subject, rectification, deletion or limitation of processing or the right to object to the processing, as well as the right to transfer data;
- if processing takes place pursuant to Art. 6(1) 1 letter a) or Art. 9(1) 2 letter a) – information about the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal,
- information about the right to lodge a complaint with the supervisory authority,
- information whether the provision of personal data is a statutory or contractual requirement or a condition for concluding a contract and whether the data subject is obliged to provide it and what are the possible consequences of failure to provide the data,
- information about automated decision-making, including profiling (...).

More: <https://uck.pl/polityka-prywatnosci/przetwarzanie-danych-osobowych.html>

INFORMATION SECURITY



INFORMATION SAFETY

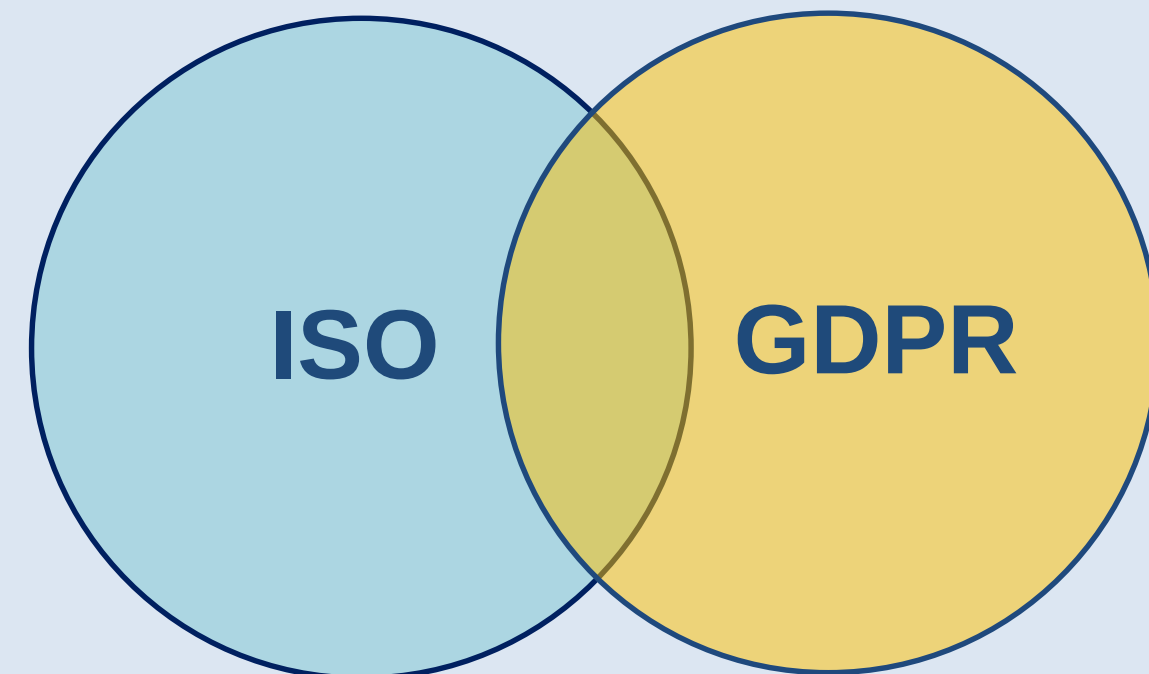
- maintaining confidentiality, integrity and availability of information. Additionally, other information properties (attributes) may be taken into account, such as authenticity, accountability, non-repudiation and reliability.



INFORMATION SECURITY ORGANIZATION. AREAS OF ACTION

Information security - areas of activity:

- Information classification
- Physical and environmental security
- ICT security (including UCK cybersecurity)
- Information security in human resources management (personal security)
- Management of ISMS incidents and weaknesses
- Risk management
- Business continuity management
- Ensuring compliance with the law of processing



STRUCTURE OF ISMS SYSTEM, STRUCTURE OF DATA PROTECTION SYSTEM

STRUCTURE OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Top Management

The Information
Security Team

Representative of the Chief Executive Officer for ISMS

Resource/assets owners - they are at the same time Risk Owners
(e.g. organizational unit (OU) managers, holders of independent
positions)

Resource/assets administrators

Other employees

ISO/IEC 27001 standard

STRUCTURE OF DATA PROTECTION SYSTEM

Personal Data Administrator (PDA)

Data Protection Officer

Authorised employees
They process personal data in accordance with the authorisation
granted by the Data Controller (to the extent justified by the duties
performed)

GDPR

INFORMATION RESOURCES/ASSETS

All information in the possession of the UCK regardless of its classification and level of protection.

Information resources include both information processed in IT systems and in traditional form.

Information assets include, for example:

- system documents (e.g. records, instructions and procedures),
- information resulting from the process (e.g. advertising, lists, databases, forms, etc.),
- information obtained at the input (e.g. from customers, from external companies, from other departments),
- information transferred to other processes (output).

A list of the UCK's information assets is maintained.



PERSONAL SECURITY



I
Activities before
employment or cooperation

II
Activities related to taking
up employment or
cooperation

III
Activities related to
modification of
employment or cooperation

IV
Activities related to the
termination of employment
or cooperation

PZ-ZI-06 –
"Information
security in
human resources
management"

INFORMATION SECURITY REQUIREMENTS BEFORE EMPLOYMENT / COOPERATION



- Confidentiality statement
- Information security training
- Authorization to process personal data

- Entrusting the processing of personal data, personal data entrustment agreement
- Confidentiality agreement
- Checklist – safety requirements
- List of sample contract clauses
- Information security guide (for the contractor)

- Putting assets into use
- Granting access rights

AUTHORIZED EMPLOYEES

Declaration

of knowledge of and compliance with the laws and rules relating to the protection of information, including personal data, and of the confidentiality of that information.



The controller and the processor shall take steps to ensure that any natural person acting under the authority of the controller or processor, who has access to personal data, shall process them **only on instructions from the controller**, unless required to do so by Union or Member State law.

Training

Authorisation to process personal data



AWARENESS, EDUCATION AND TRAINING IN THE FIELD OF INFORMATION SECURITY

Persons/entities who, in connection with the tasks they perform, gain access to information UCK assets:

- have appropriate knowledge in the field of information security (i.e. have a level of information security awareness appropriate to the position held/tasks performed),
- they know recommendations and methods for the proper use and protection of information systems.

Granting access to the UCK's information assets, in particular information and information processing means, takes place only after documented submission of appropriate information security rules applicable in the UCK.

BASIC TRAINING

ADDITIONAL TRAINING (adapted to the tasks entrusted), the completion of which is a condition for obtaining access to: individual UCK information resources, including ICT systems processing data, advanced functionalities of ICT UCK systems.

INITIAL TRAINING
PERIODIC TRAINING
REFRESHING TRAINING



PHYSICAL AND ENVIRONMENTAL SECURITY

<p>Physical security of entrances (securing entrances to buildings and rooms)</p>	<p>Access Control</p>	<p>Protection against external threats (protection against the forces of nature and the actions of third parties, e.g. walls, partitions, appropriate location of office furniture)</p>
<p>Securing the premises by employees (duty of securing the premises, where protected information is being held)</p>	<p>Secured area (Designated area for processing of information/personal data, security zones, working in a secure area)</p>	<p>Securing of information carriers by employees (obligation to secure information carriers containing protected information)</p>
<p>Clean desk policy, clean whiteboard policy (rules for maintaining a clean desk and clean board policy during and after work)</p>	<p>Surveillance of persons (supervision of persons not authorised to process information, e.g. patients, contractors)</p>	<p>Key policy (key surrender, supervised storage, prohibition of taking the keys to UCK premises home)</p>



RESPONSIBILITY FOR RESOURCES/ASSETS



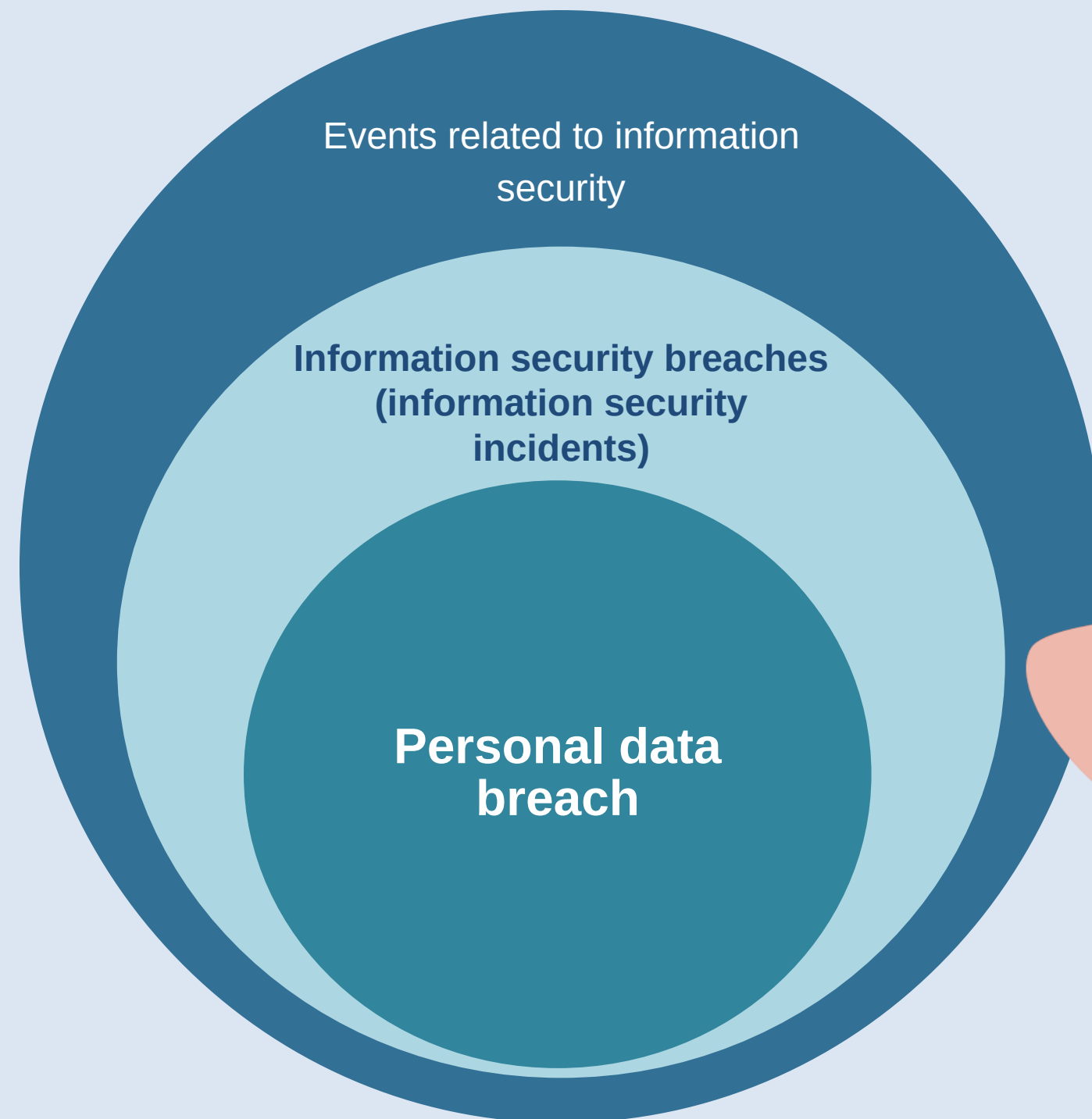
Each employee is responsible for the resources/assets entrusted to him/her (IT equipment, software, paper documentation, etc.).

Each employee is required to pay particular attention to the security of the processed information, in particular against unauthorized access and destruction. Each employee is required to exercise particular care during **transport, storage and use** of the information carrier.

These resources/assets are - as a rule - intended only **for official purposes**. Their use for private purposes is only possible in cases defined by UCK internal regulations.

ISMS INCIDENT AND WEAKNESS MANAGEMENT.

EVENTS RELATED TO INFORMATION SECURITY



Events related to information security are:

- information security breaches,
- other events that do not have the characteristics of information security breaches (weaknesses in the ISMS).



Weaknesses in the ISMS can lead to information security breaches.

BUSINESS CONTINUITY MANAGEMENT

Business Continuity Plans (BCP)

Business continuity - the strategic and tactical ability of an organization to anticipate and respond to crisis situations, enabling the continuation of business processes at an acceptable, predefined level within an acceptable time.

Business continuity management - a management process that aims to ensure the uninterrupted implementation of the organization's services at the assumed level (including the identification of events that may lead to a crisis situation or disruption to business continuity and their impact on business processes and the implementation of appropriate measures needed to ensure UCK business continuity). This process provides a structure on which the institution's resilience is built, with the ability to respond effectively, and which protects the interests of key stakeholders as well as the institution's reputation, brand and value-creating activities. Business continuity management aims to ensure (by establishing a process and organizing operations) that a certain level of operational performance considered to be the minimum necessary will be maintained even in conditions of critical disruption.



Reviewing, testing and assessing
Business Continuity Plans (BCP)

DPO STATUS (ARTICLE 38 GDPR)

The personal data controller and the Processor ensure that **the DPO is properly and promptly involved in all matters relating to the protection of personal data** (the DPO should be informed about all issues relating to the processing of personal data at the earliest possible stage).

The personal data administrator and the Processor **support the DPO in fulfilling the tasks** referred to in Art. 39 GDPR, providing him with the resources necessary to perform these tasks and access to personal data and processing operations, as well as the resources necessary to maintain his professional knowledge (including appropriate financial, infrastructural and human resources support, as well as ensuring participation in training, workshops, forums and other meetings on personal data protection, as well as providing him with appropriate professional literature to update his knowledge, including industry magazines).

The personal data controller and the processor ensure that the **DPO does not receive instructions** regarding the performance of these tasks (e.g. the DPO should not be given instructions on how to interpret the provisions and/or on how to formulate recommendations and opinions); he is not dismissed or punished for fulfilling his duties; should report directly to the Top Management (independence of the DPO).

Data subjects **may contact the Data Protection Officer** in all related matters with the processing of their personal data and with the exercise of their rights under the GDPR.

The DPO is **obliged to maintain secrecy or confidentiality regarding the performance of his tasks** - in accordance with EU or national law.

The DPO may perform other tasks and duties; The personal data controller and the processor shall ensure that such tasks and responsibilities do not result in a conflict of interests.



DPO OBLIGATIONS (ARTICLE 39 GDPR)

Consultative, informative, advisory and monitoring role

Informing the Personal Data Administrator, the Processor and employees who process personal data about their obligations under the GDPR and other regulations (...) and advising them on this matter (...).

Monitoring compliance with the GDPR, other regulations (...) and the policies of the Personal Data Administrator or Processor in the field of personal data protection (...).

Providing recommendations on the data protection impact assessment upon request and monitoring its implementation in accordance with Art. 35 GDPR (...).

Cooperation with the Supervisory Authority (the President of the Personal Data Protection Office), including participation in inspections regarding the processing of personal data.

Acting as a contact point for the Supervisory Authority on matters related to processing, including prior consultations referred to in Art. 36 GDPR and, where appropriate, conducting consultations on any other matters.



CONTACT WITH THE DATA PROTECTION OFFICER

DATA PROTECTION OFFICER MONIKA GOLUBSKA

☎ tel. (58) 349 21 73

✉ iod@uck.gda.pl

