Personal data protection

Basic terminology and information

Personal data (Art. 4 section 1 of the GDPR)

Personal data – information concerning 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:

- name and surname
- identification number
- location data
- Online identifier
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data – analysis

Personal data – refers to information [...]

Information:

- communication (regardless how it is recorded)
- characters, words, sounds, photographs, x-rays, DNA...

Personal data – analysis

Personal data – information [...] concerning a natural person

Natural person:

~~Company KRS no., REGON no.~~
~~legal person name~~
~~fictitious character (House M.D.)~~ (unlike the actor who plays him)

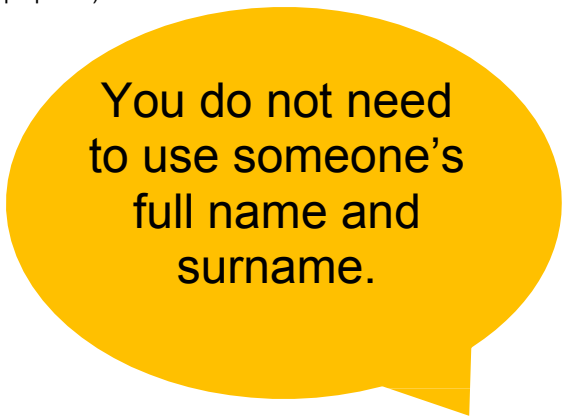
- Monika Golubska

Personal data – analysis

Personal data – any information relating to an identified or identifiable natural person.

Examples of identified or identifiable persons:

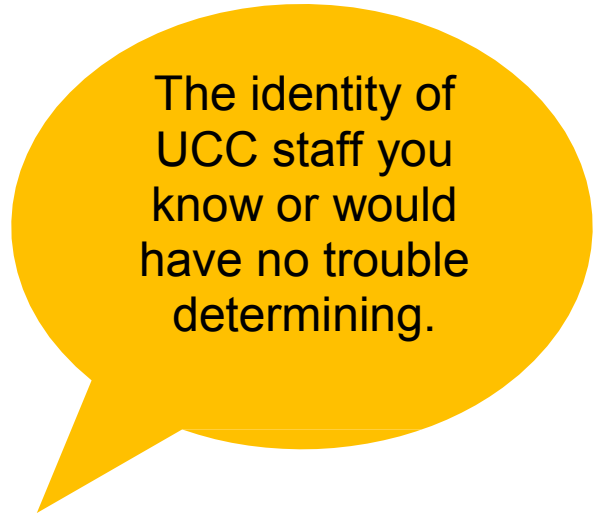
- owner of building no. 10 on Kwiatowa St. in Warsaw (fictitious data for training purposes)
- long-time owner of the bar on Grudziądzka St. in Warsaw (fictitious data for training purposes)
- Ms. Zofia, employee of PKO BP's office in Gdańsk on Azaliowa St. (fictitious data for training purposes)
- owner of the "Stokrotka" club in Zaspa, Gdańsk's (fictitious data for training purposes)
- the author of 'Salem's lot'
- Lech, 1983 Nobel Peace Prize winner
- Katarzyna T., blogger, daughter of a former Prime Minister
- Tomasz P., former Mayor of Gdańsk.
- the vocalist of the band "Dżem"
- Renata B., member of the Sejm
- PESEL no.



Personal data – analysis

Examples of identified or identifiable persons at UCC:

- Head of the UCC Adult Psychiatry Clinic
- UCC Data Protection Officer
- Wioletta, responsible for the UCC Integrated Management System
- Edyta, member of the UCC Human Resources Division
- mgolubska@uck.gda.pl
- Monika, responsible for personal data protection at UCC
- Managing Director of UCC
- Jakub K., Director of UCC



Personal data (official interpretation)

The General Data Protection Inspector (GIODO, the former supervisory body), based on previously-binding provisions, considered personal data to mean “information relating to any aspect of a person’s professional or private life, education, knowledge or character” (GIODO ruling of 26 November 2009, Dolis/DEC-1183/09).

Does the GDPR apply to the deceased?

Recital 27 of the GDPR:

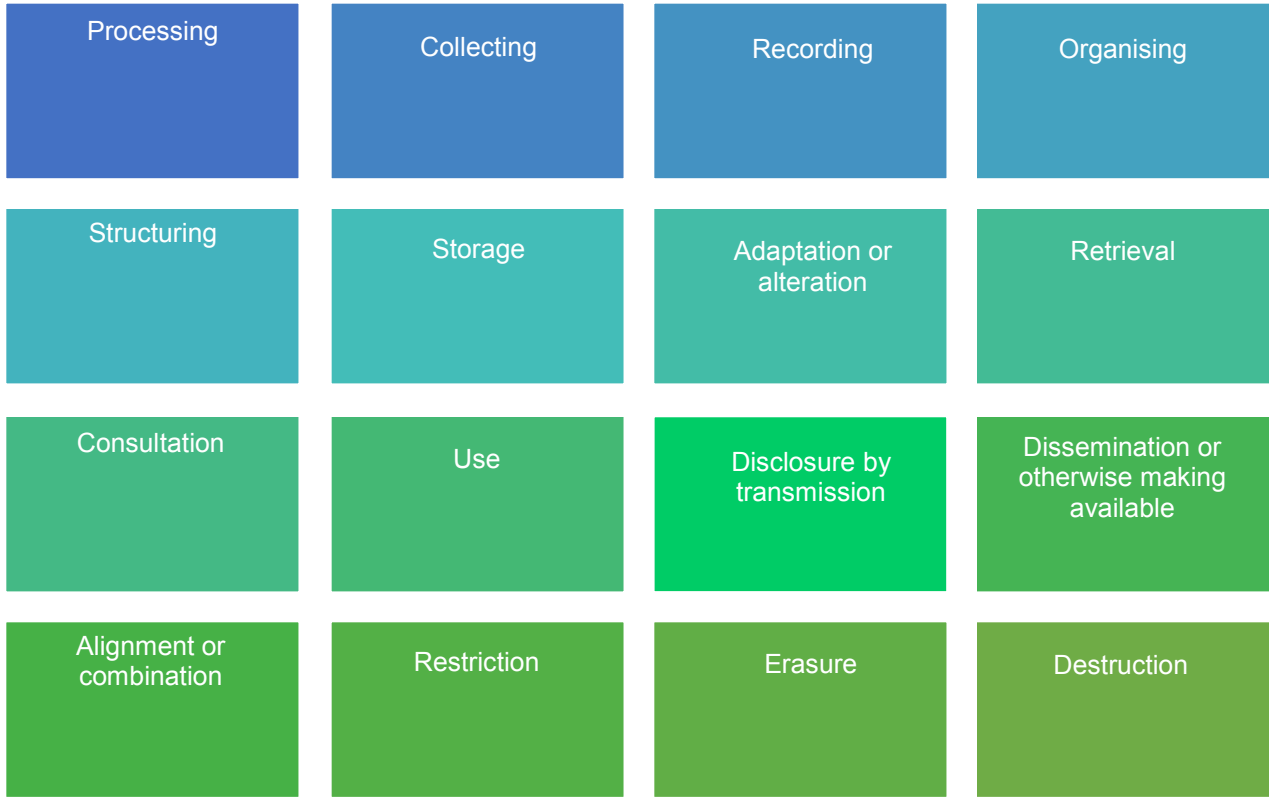
The GDPR does not apply to the personal data of deceased persons. Member states may adopt regulations on the processing of the personal data of deceased persons.

Conclusions:

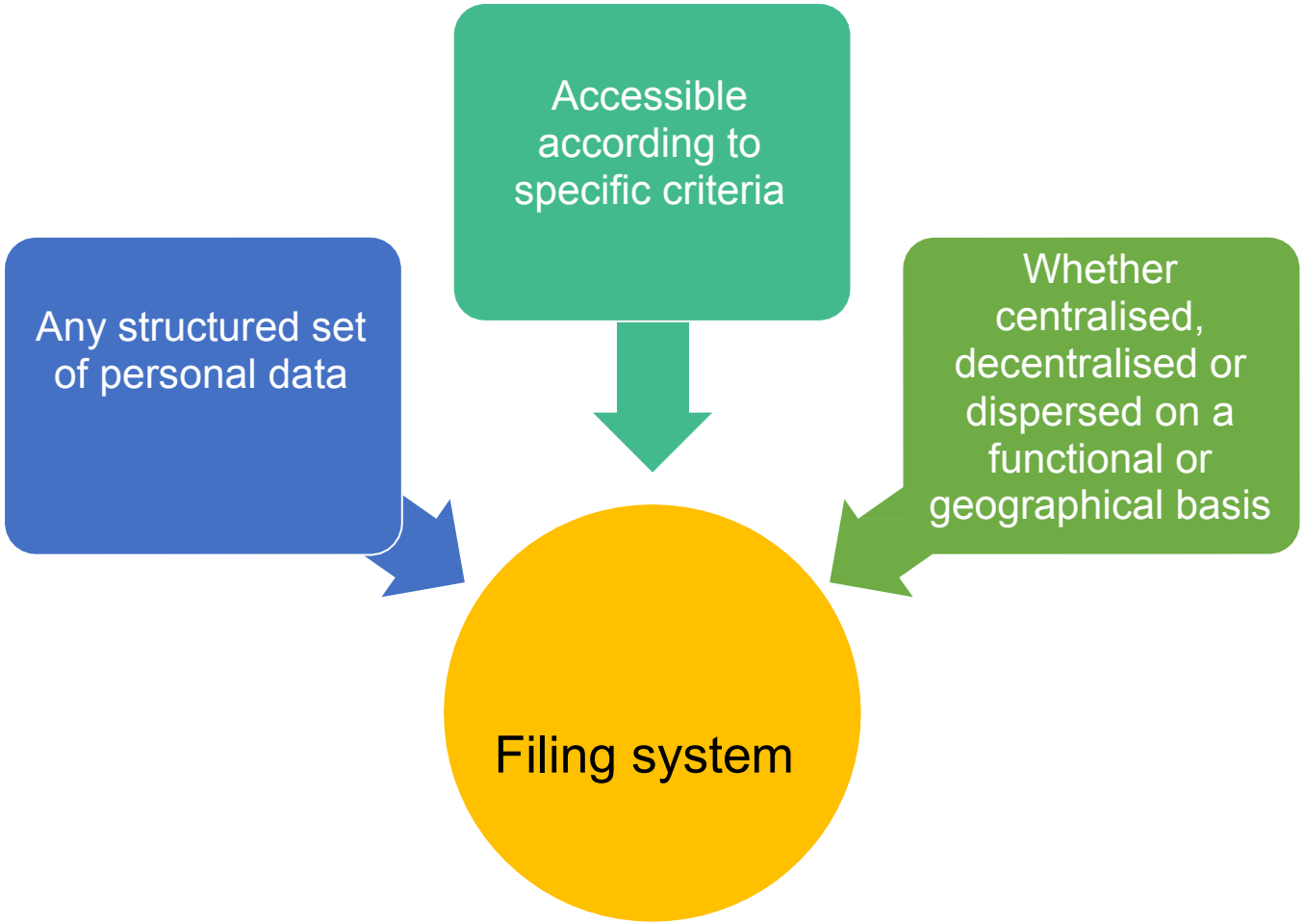
- refusal to share data relating to deceased persons by invoking the GDPR must be considered baseless (the GIODO expressed a similar opinion based on the now-repealed act on personal data protection),
- in the case of using the personal data of a deceased person (e.g. sending advertising pamphlets addressed to a deceased person), his or her relatives whose personal interests, i.e. the memory of the deceased person, is infringed upon have the right to bring a civil action to court.

Processing (Art. 4 section 2 of the 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:



Filing system (Art. 4 section 6 of the GDPR)



Supervisory Authority (Art. 4 section 21 of the GDPR)

Supervisory Authority – means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.

In Poland, it is the President of the Personal Data Protection Office (PUODO).

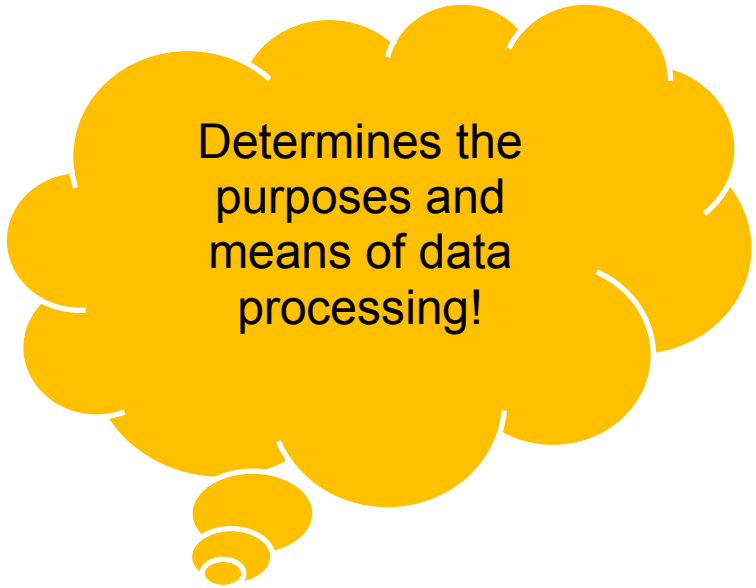
Controller (Art. 4 section 7 of the GDPR)

Controller – means the 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 [...]

Hospital

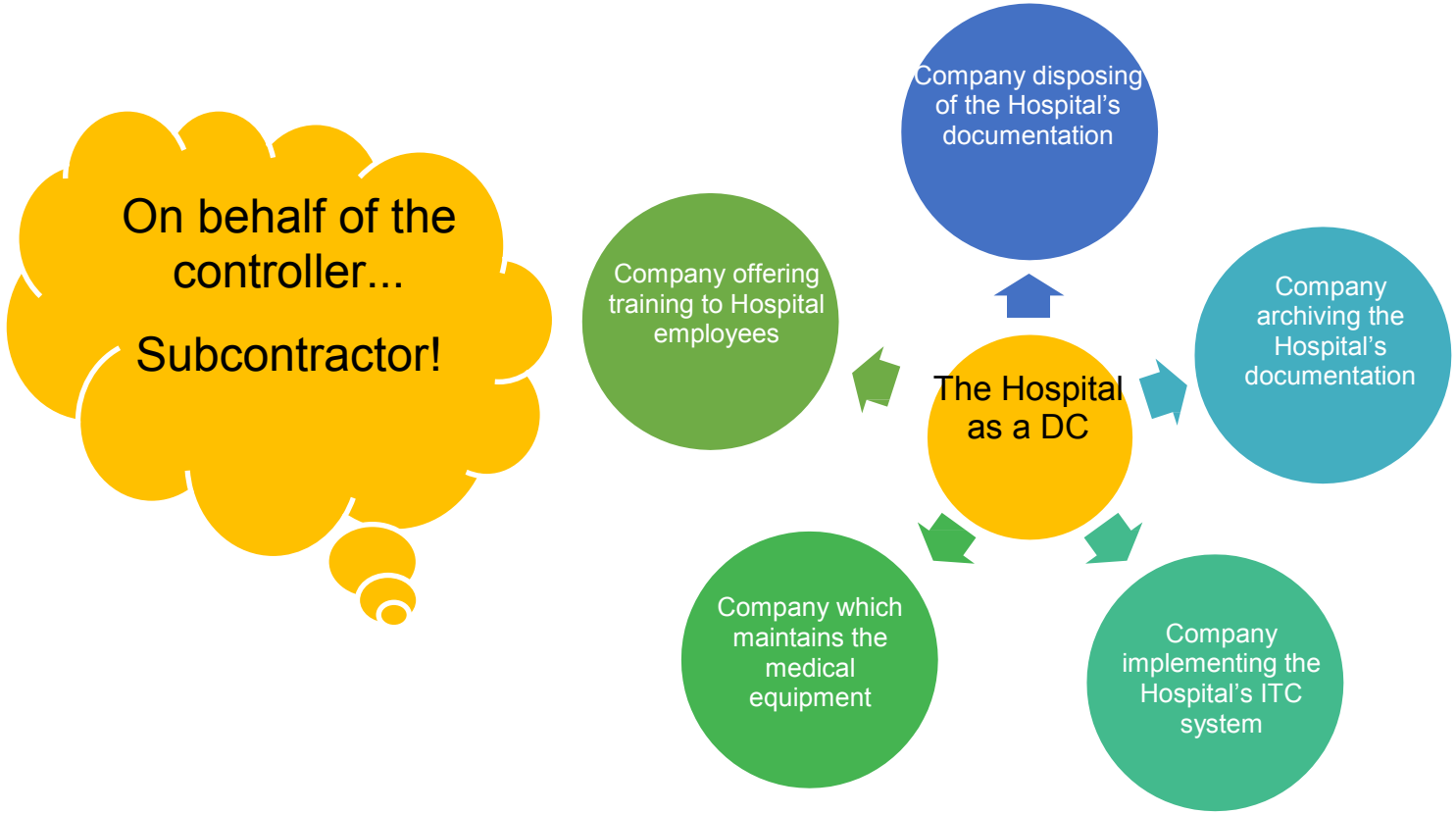
Company owner

Mayor



Processor (Art. 4 section 7 of the GDPR)

Processor – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.



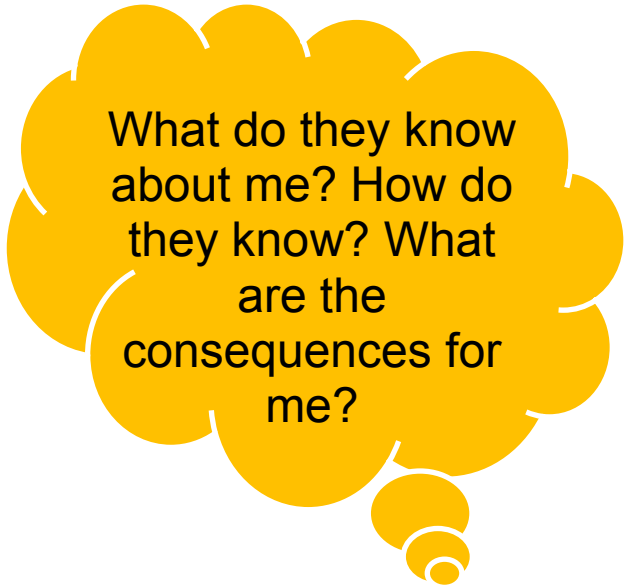
Data Recipient, Third Party (Art. 4 sections 9 and 10 of the GDPR)

(Data) Recipient – means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry [...] shall not be regarded as recipients [...]

Third Party – means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Profiling (Art. 4 section 4 of the GDPR)

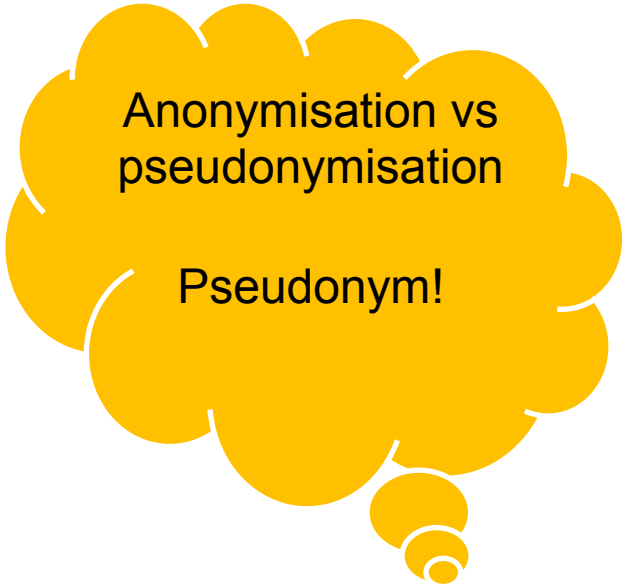
Profiling – means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict



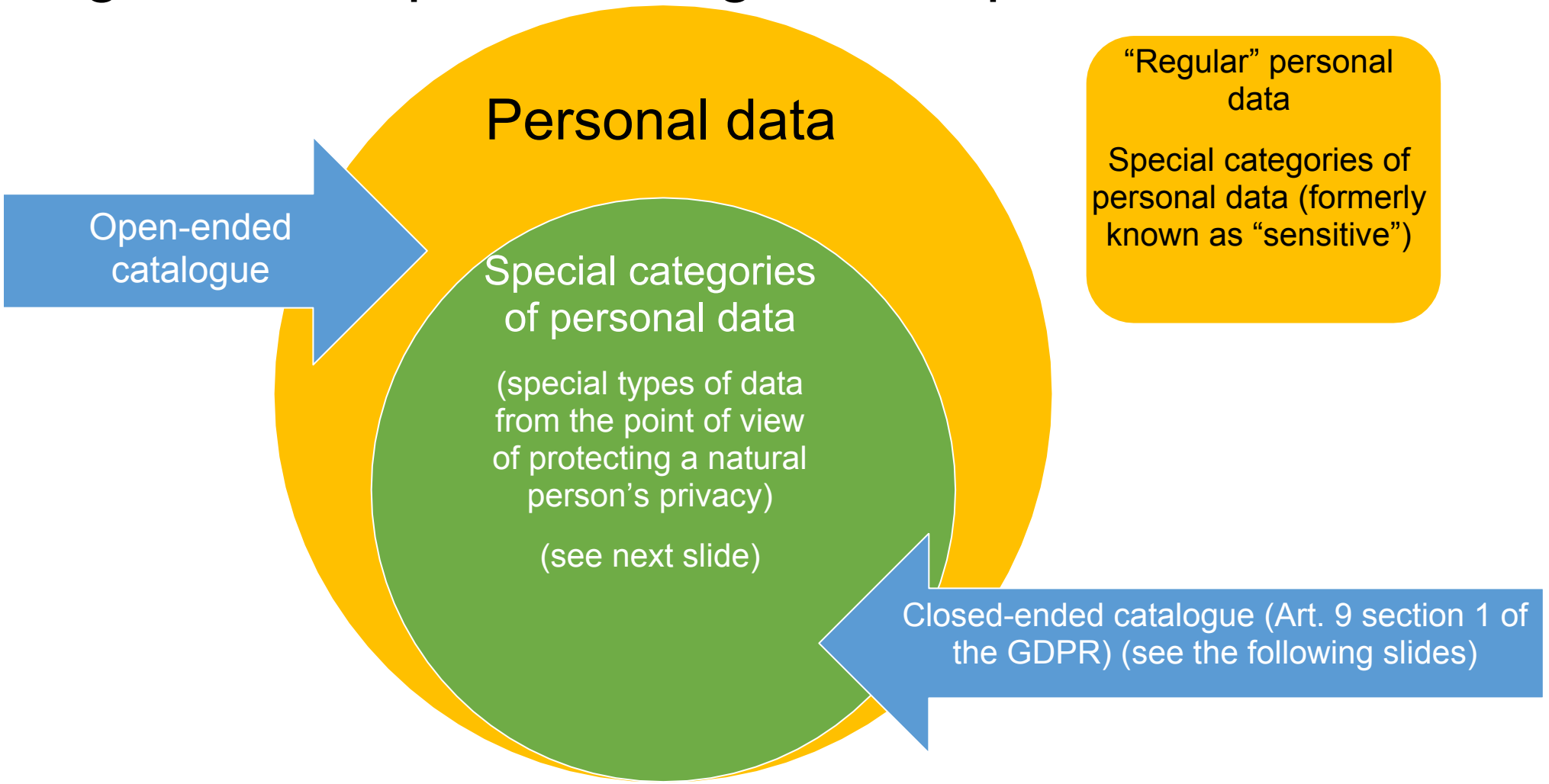
- aspects concerning that natural person's performance at work
- economic situation
- health
- personal preferences
- interests
- reliability
- behaviour
- location
- movement

Pseudonymisation (Art. 4 section 5 of the GDPR)

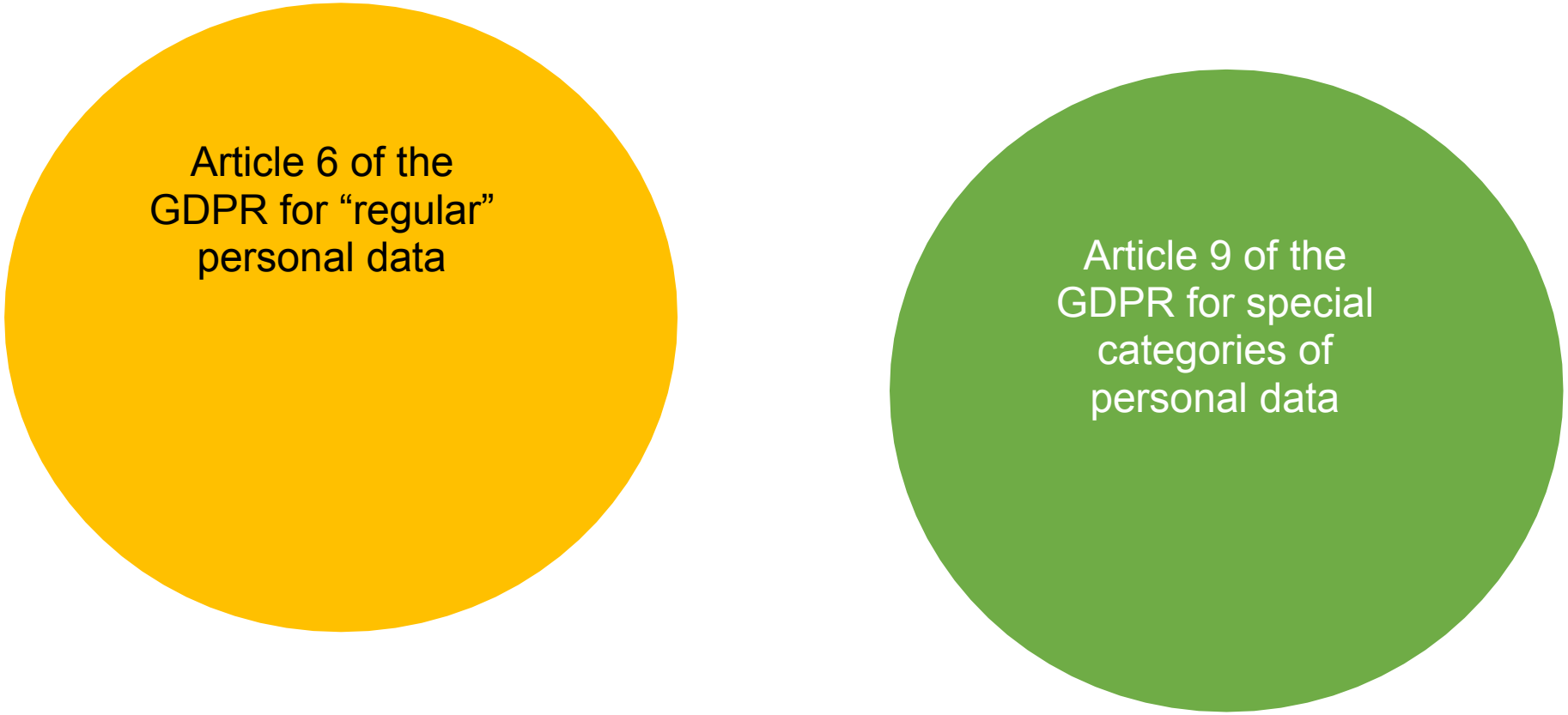
Pseudonymisation – means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.



Regular and special categories of personal data



Lawfulness of processing



“Regular” personal data (Art. 6 of the GDPR)

Art. 6 section 1 of the GDPR: Processing 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 categories of personal data (Art. 9 of the GDPR)

Art. 9 section 1 of the GDPR: Processing of the following types of personal data shall be prohibited:

- data revealing racial or ethnic origins
- data revealing political opinions
- data revealing religious or philosophical beliefs
- data revealing trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

On principle, processing of special categories of personal data is prohibited

Closed-ended catalogue of special categories of data

Special categories of personal data (Art. 9 of the GDPR)

Art. 9 section 2 of the GDPR: Art. 9 section 1 of the GDPR [concerning the prohibition of processing special categories of personal data] does not apply if:

Lifting of the prohibition on the processing of special categories of personal data

a) the data subject has given explicit consent [...], except where Union or Member State law provide that the prohibition [...] may not be lifted by the data subject.

b) 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 [...]

c) 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

d) 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 [...]

Special categories of personal data

e) processing relates to personal data which are manifestly made public by the data subject

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) 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

h) 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 of the GDPR

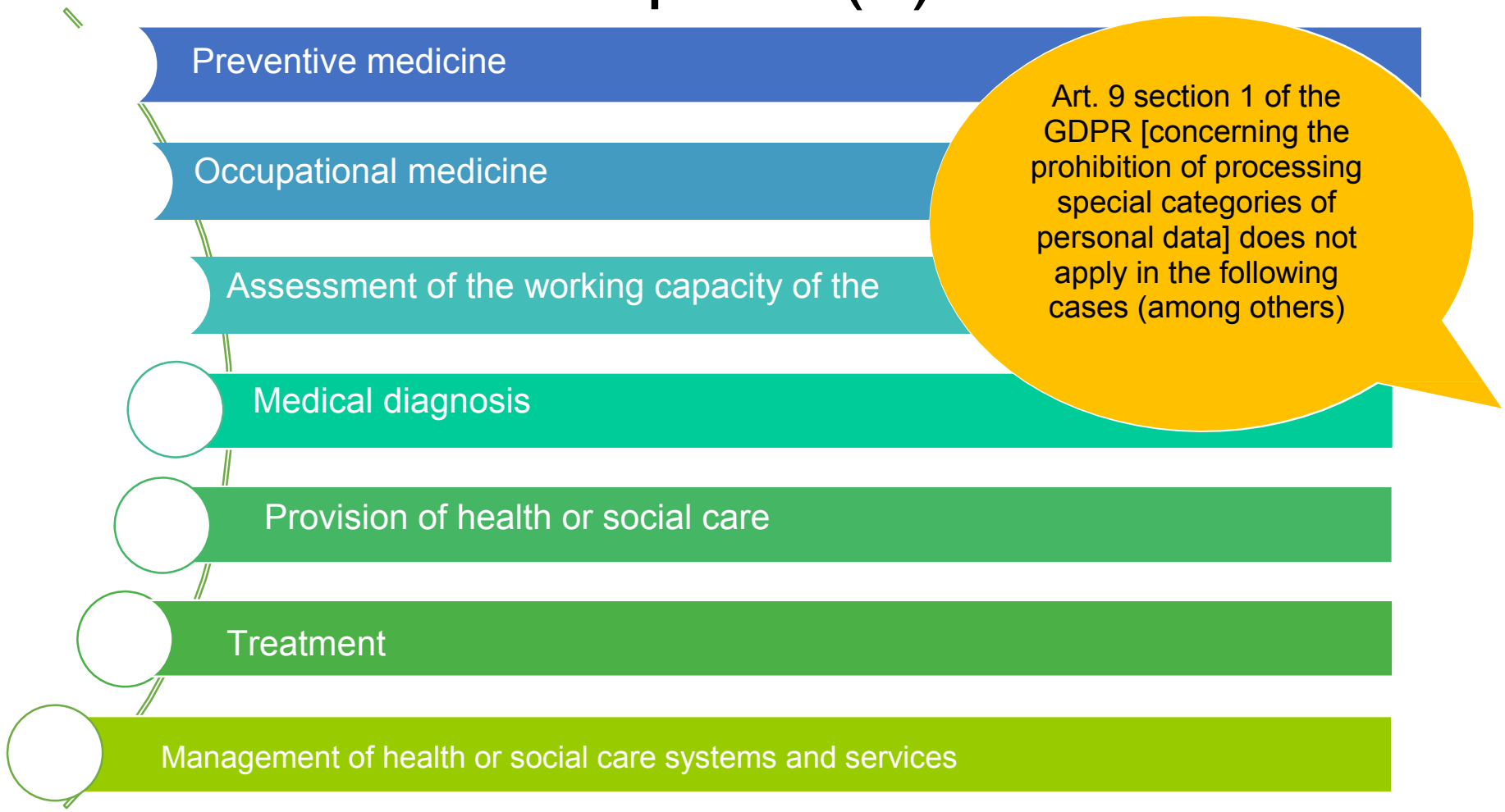
An additional reference to this goal is made in Art. 9 section 3 of the GDPR

Special categories of personal data

i) 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

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [...]

Art. 9 section 2 point (h) of the GDPR

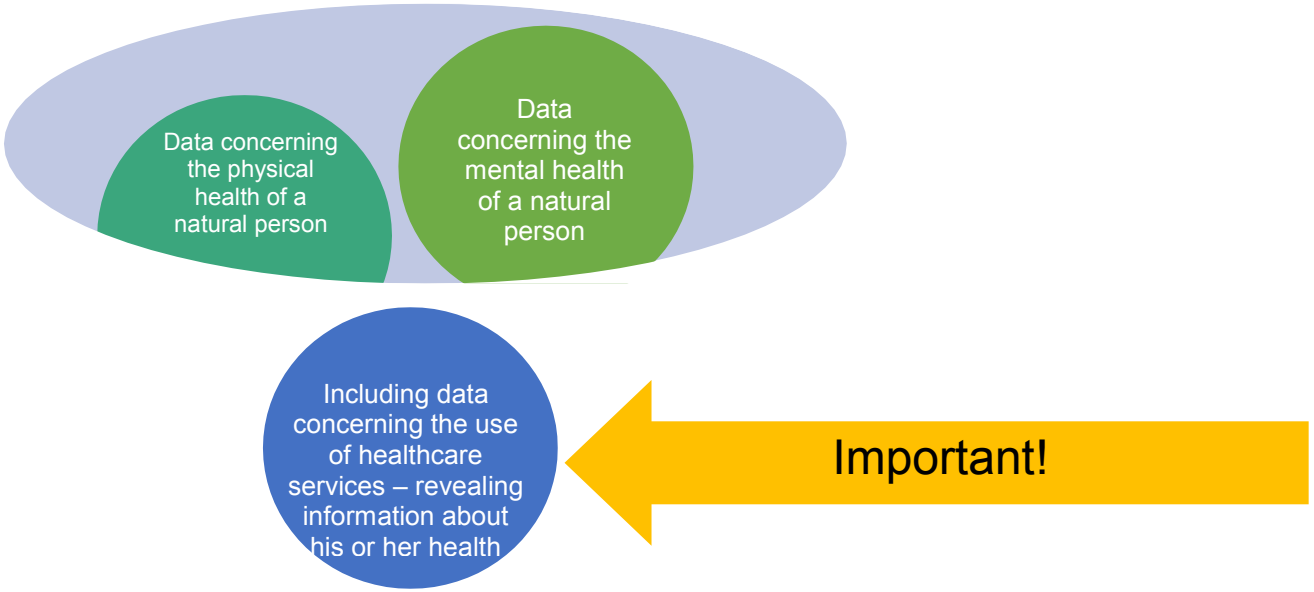


Art. 9 section 3 of the GDPR

Personal data referred to in Art. 9 paragraph 1 of the GDPR [special categories of personal data] may be processed for the purposes referred to in point (h) of paragraph 2 Art.9 of the GDPR [health care] when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

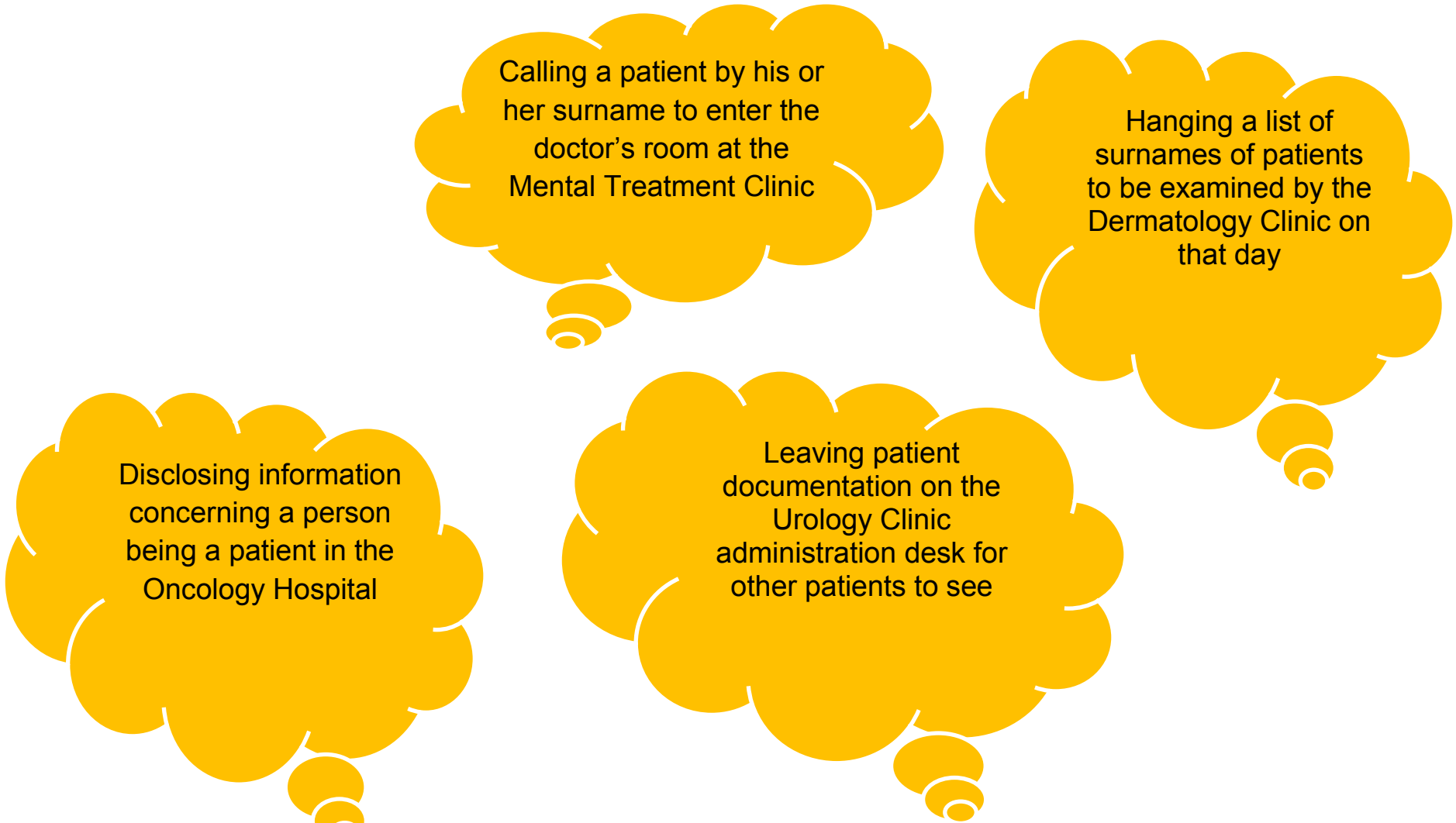
Error in the Polish translation of the GDPR. The word “occupational” does not appear in the original.

Data concerning health (Art. 4 section 15 of the GDPR)



Data concerning health

Data concerning health (Art. 4 section 15 of the GDPR)

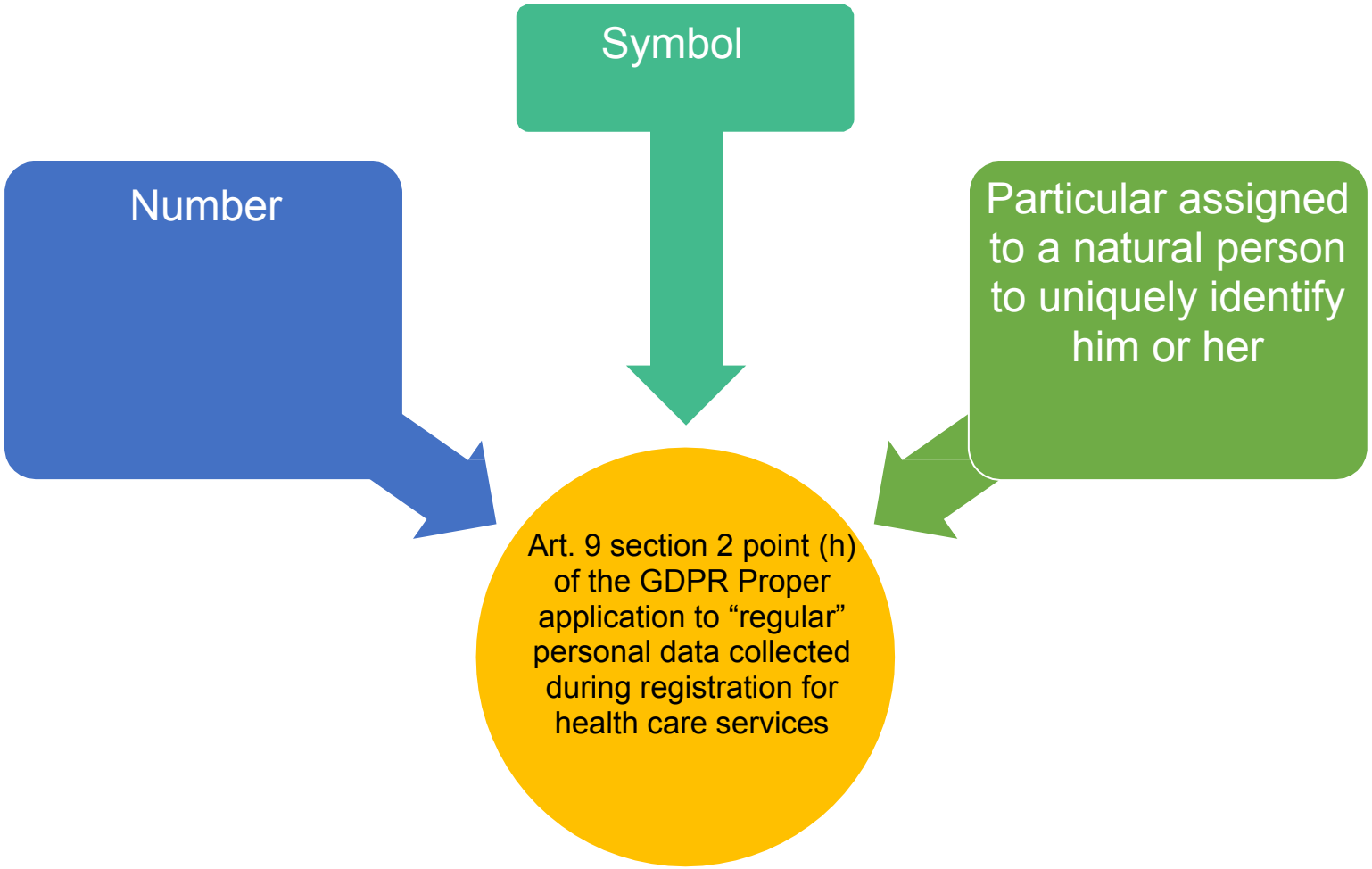


Recital 35 of the GDPR

Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.

This includes information about the natural person collected in the course of the registration for, or the provision of, health care services [...] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Recital 35 of the GDPR



Genetic data, biometric data (Art. 4 sections 13 and 14 of the GDPR)

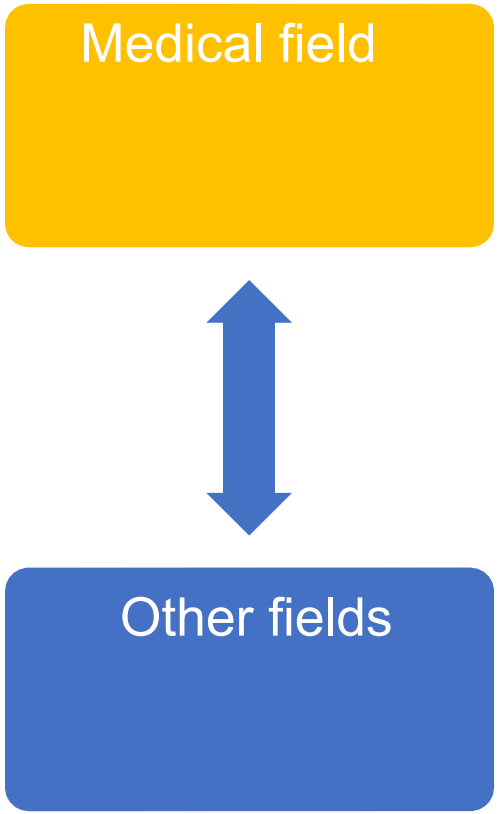
Genetic data – means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

Biometric data – means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

Art. 9 section 4 of the GDPR

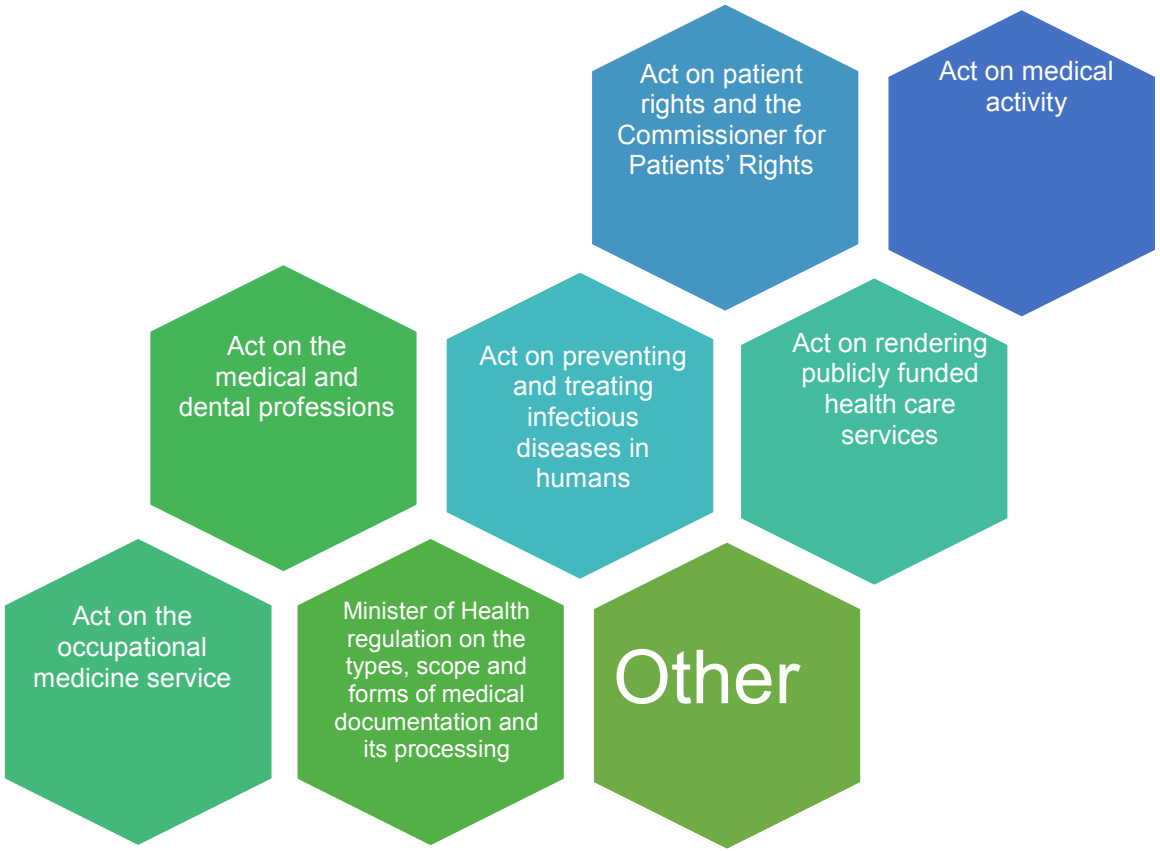
Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Polish legal bases for the processing of health status data



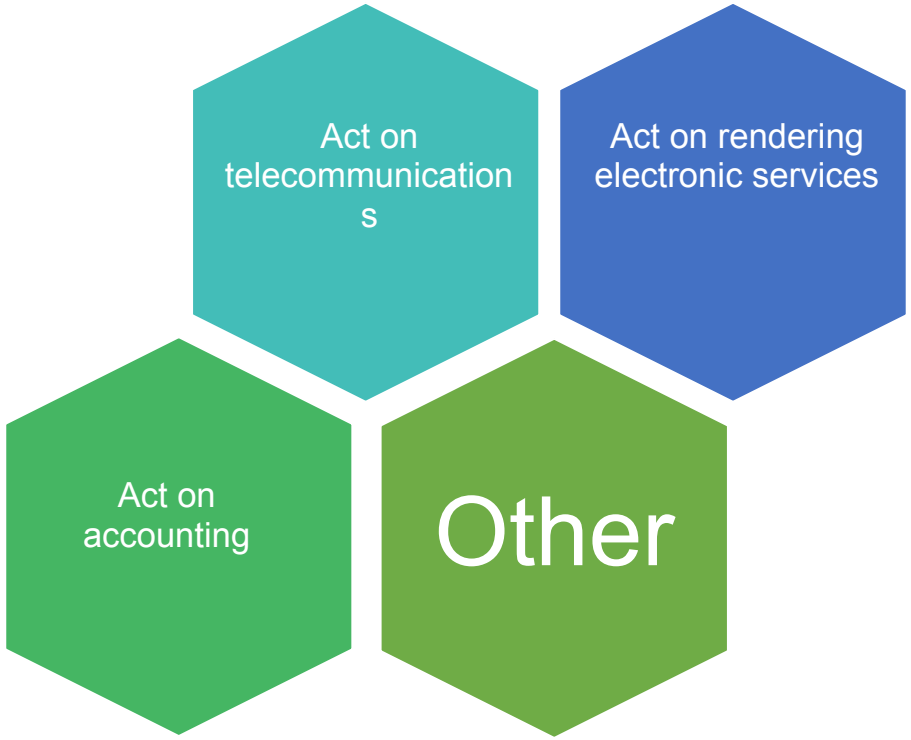
Processing of health status data: legal regulations

MEDICAL FIELD



Processing of health status data: legal regulations

OTHER FIELDS



Rights of data subjects

- Right to information and to access personal data: Art. 13-15 of the GDPR:
- Art. 13 of the GDPR – Information to be provided where personal data are collected from the data subject
- Art. 14 of the GDPR – Information to be provided where personal data have not been obtained from the data subject
- Art. 15 of the GDPR – Right of access by the data subject

- Right to rectification: Art. 16 of the GDPR
- Right to erasure (right to be forgotten): Art. 17 of the GDPR
- Right to restriction of processing: Art. 18 of the GDPR
- Right to data portability: Art. 20 of the GDPR
- Right to object: Art. 21 of the GDPR

Responsibility of the Controller (Art. 24 of the GDPR)

Responsibility of the Controller:

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Where proportionate in relation to processing activities, the measures referred to above shall include the implementation of appropriate data protection policies by the controller.

Adherence to approved codes of conduct as referred to in Article 40 of the GDPR or approved certification mechanisms as referred to in Article 42 of the GDPR may be used as an element by which to demonstrate compliance with the obligations of the controller.

Privacy by design (Art. 25 section 1 of the GDPR)

Privacy by design

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Privacy by default (Art. 25 section 2 of the GDPR)

Privacy by default

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

That obligation applies to:

- the amount of personal data collected,
- the extent of their processing,
- the period of their storage and
- their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Security of processing (Art. 32 of the GDPR)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

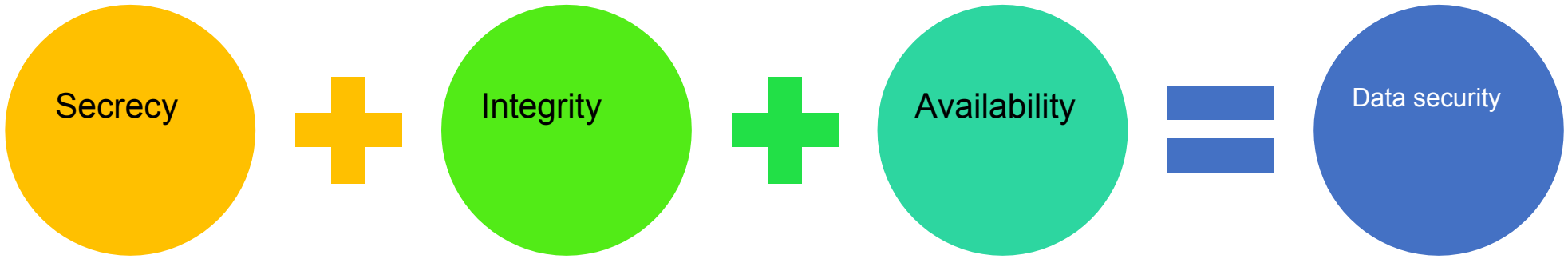
- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Security of processing (Art. 32 of the GDPR)

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

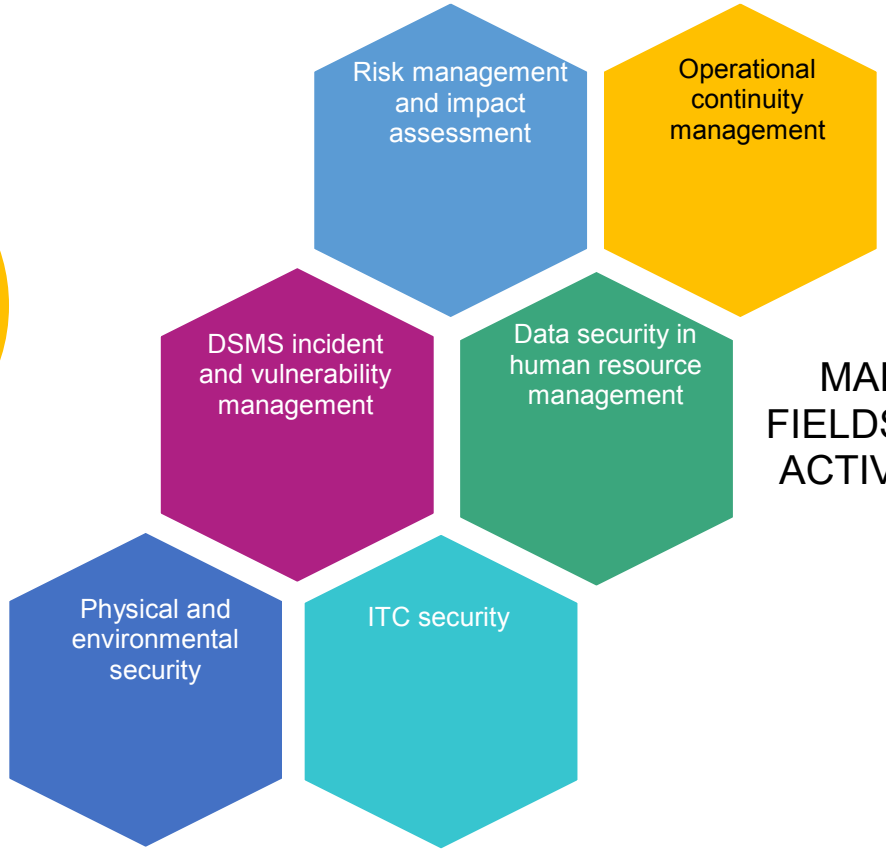
Security of processing



Security of processing

A number of **obligations imposed on UCC staff** by the procedures of the Integrated Management System (IMS), in particular in the procedures of the **Data Security Management System (DSMS)**

(PZ, PZ-ZI)



MAIN FIELDS OF ACTIVITY

Personal data breach (Art. 4 section 12 of the GDPR)

Art. 4 section 12 of the GDPR

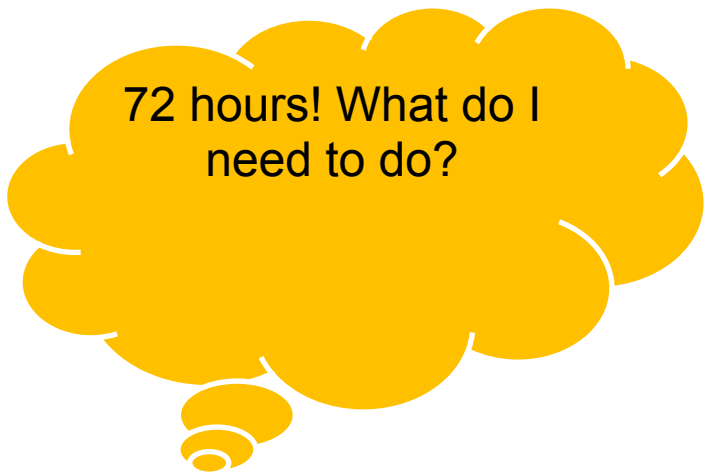
Personal data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Reporting breaches to the Supervisory Authority

Art. 33 sections 1 and 2 of the GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.



Breach reporting exceptions

It is not required to inform data subjects about a breach if:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects [...] is no longer likely to materialise
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Informing data subjects about a breach

Recital 86 of the GDPR

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions.
The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects.
Such communications [...] should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

Liability for breaches

Administrative liability
administrative monetary penalty in the form of up to EUR 20 million or 4% of the company's entire global turnover of the preceding fiscal year – whichever is higher

UODO: public entities – up to PLN 100,000

Criminal liability

Compensatory liability

Disciplinary liability

Thank you for your attention

Monika Golubska

Representative of the Managing Director for the Data Security Management System

Data Protection Officer

mgolubska@uck.gda.pl Phone: 58 349 21 73