**Order no 17/2022**

**of the Rector of the Medical University of Bialystok**

**of 8.03.2022**

**on the processing of personal data of specific categories for the purposes of scientific research**

Based on: art. 469b of the Law of July 20, 2018 Law on Higher Education and Science (i.e. Journal of Laws from 2021 pos. 478, as amended)*,* art. 24 of the Regulation of the European Parliament and Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to   
with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC, hereinafter referred to as the GDPR, I hereby order the following:

# § 1

# General principles

1. The terms used in the content of the order have the following meaning:
2. personal data - information about an identified or identifiable natural person (the "data subject"); an identifiable natural person is a person who can be identified directly or indirectly, in particular by means of an identifier such as a name   
   and surname, identification number, location data, internet identifier or one or more specific factors determining the physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person;
3. data of specific categories – personal data revealing racial or ethnic origin, political views, religious or worldview beliefs, trade union membership and genetic data, biometric data clearly identifying a natural person, data concerning health, sexuality or sexual orientation;
4. genetic data – personal data relating to the inherited or acquired genetic characteristics of a natural person that reveal unique information   
   on the physiology or health of that person and which result in particular from the analysis of a biological sample taken from that natural person;
5. health data - personal data on the physical or mental health of a natural person, including the use of health care services-revealing information about his or her state of health, these should include data revealing information about the past, present or future state of physical or mental health of the data subject. This includes personal data, e.g. collected during the performance of laboratory diagnostics services provided by the University, information from laboratory or medical examinations of body parts or body fluids, including genetic data and biological samples, information about the disease, disability, risk of disease, medical history, clinical treatment or physiological or biomedical condition of the data subject, regardless of their source;
6. pseudonymisation – processing of personal data in such a way that it is impossible to attribute them to a specific person to whom the data relate, without the use of additional information, provided that such additional information is stored separately and is covered by technical and organizational measures that prevent it from being assigned to an identified or identifiable natural person;
7. anonymisation - processing of personal data in such a way that it can no longer be attributed to the specific person to whom the data relate. This is an irreversible process.
8. Personal data must be:
9. processed lawfully, honestly and in a manner that is transparent to the research participant and/or his legal guardian;
10. collected for specific, explicit and legally justified purposes   
    and not further processed in a manner inconsistent with those objectives (objective limitation);
11. adequate, relevant and limited to what is necessary for the purpose of the research (data minimisation);
12. correct and, if necessary, updated; all possible steps should be taken to ensure that personal data which are incorrect in the light of the purpose of the scientific investigation are corrected without delay and, if this is not possible, deleted;
13. stored in a form which permits the identification of the data subject for no longer than is necessary for the purpose of carrying out the scientific research.   
    It is necessary to obtain additional consent from the research participant (storage restriction) for the storage of personal data with the possibility of their use   
    in the future;
14. processed in a manner that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organisational means, including   
    in particular, the principles set out in this Order (integrity   
    and confidentiality).
15. The course of the research should be designed in a way  that limits processing of personal data.  
    to the necessary minimum
16. Personal data shall be anonymised as soon as the purpose of research or development has been achieved. Until then, the data that enables the identification of the research participant shall be recorded separately. It may only be combined with specific information relating to a person if the purpose of research or development requires so.
17. Publication of research results and works takes place in a way that prevents identification of the research participant, through anonymisation or pseudonymisation, both in terms of text studies and apparatus results (the so-called source data), and making it impossible to identify a person in paintings and figures.
18. When collecting data through electronic surveys, use the functionality and systems provided by the University. Where other systems are used, it should be ensured that the possibility for partners to use and share data for other purposes without consent   
    and knowledge of the researcher is limited. When using other systems not authorized by the University in the case of the transfer of personal data, the agreement referred to in art. 28 GDPR should be concluded
19. When processing all kinds of data for scientific purposes, internal legal acts on data protection shall apply.
20. Any incidents related to the security of specific categories of scientific and research personal data, in particular the loss of their confidentiality, availability or integrity, should be reported immediately to the Data Protection Officer.
21. Employees processing personal data of specific categories in scientific and research work are obliged to participate in training on data protection conducted by the University's Data Protection Officer.

# § 2

# Data Protection Impact Assessment

1. If a given type of personal data processing for scientific purposes, in particular with the use of new technologies - due to its nature, scope, context and objectives,   
    is likely to result in a high risk of violating the rights or freedoms of natural persons, the Researcher, prior to the processing, assesses the effects of the planned processing operations for the protection of personal data.
2. When assessing the impact on data protection, the Researcher consults the university's Data Protection Officer.
3. The assessment referred to in paragraph 1 shall be carried out taking into account any requirements described in art. 35 GDPR in accordance with the rules defined in a separate regulation.

# § 3

# Personal data protection

1. Personal data processed for scientific purposes shall be protected by appropriate technical and organisational measures, taking into account the current state of technical knowledge, the cost of implementing the security and the nature, scope, context and purposes of the processing, and the risk of violating the rights or freedoms of natural persons of varying likelihood and severity, in order to ensure a degree of security corresponding to that risk.
2. When processing personal data, appropriate technical and organizational security for the rights and freedoms of natural persons whose personal data are processed, in accordance with the GDPR Regulation, shall be implemented, in particular by:
   1. pseudonymisation or encryption of data,
   2. granting authorization to process them to a minimum number of people necessary to conduct research and development works,
   3. control of access to premises where documents containing personal data are stored,
   4. securing personal data in paper form in lockers with a patent lock,
   5. encryption of personal data in electronic form.
3. When pseudonymising the personal data of a research participant, the use of codes based on numerical personal data (e.g. PESEL number) shall be avoided.
4. In order to ensure the control of access to the premises where documents containing personal data are stored, the head of the organisational unit conducting the research shall determine how the keys to these premises are to be handed over to ensure that access is controlled against unauthorised persons.
5. In the case of the establishment of an organisational unit on the basis of a medical entity, the head of the organisational unit conducting scientific research agrees the method of controlling (recording) the access and security of the premises with the appropriate organisational unit of this medical entity.

# §4

# Exchange of research data

1. Data shall be made available to another research centre with the consent of the head of the organisational unit conducting the research on the basis of an agreement between the University and that research centre. Anonymised data may be made available without an agreement in exceptional cases and with the consent of the head of the organisational unit conducting the research, provided that it does not violate patent procedures and licensing conditions.
2. If an investigation is planned in cooperation with another external entity, the institution should consult the Data Protection Officer in order to properly regulate the protection of personal data.
3. Each signed agreement that involves the transfer of personal data (both ordinary personal data i.e. name, surname, PESEL number, etc. as well as personal data of a specific category, such as health, genetic data, biological samples that can identify a person) should:

* regulate general issues relating to the protection of personal data

and if necessary:

* conclude an additional agreement: entrusting the processing of personal data or co-administering personal data or regulating the transfer of personal data to third countries in accordance with Chapter V of the GDPR.

1. The relevant provisions governing data protection issues in the agreements and the agreement templates can be found on the University's website in the Data Protection Officer tab under the link: https://www.umb.edu.pl/iod/badania
2. The provisions of the agreements referred to in this paragraph shall not restrict the provisions of this regulation.

# § 5

# How to handle personal data of persosns directly participating in a scientific study

1. The processing of personal data requires the receipt of consent for their processing   
   from the research participant or the consent of the legal guardian or parent of a person without legal capacity participating in the research.
2. At the time of obtaining personal data from a research participant or a parent / legal guardian of a person without legal capacity, information on the processing of personal data in accordance with art. 13 and 14 GDPR should be presented
3. Templates of consents and information clauses referred to in paragraphs 1 and 2 can be found on the University's website www.umb.edu.pl/iod.

# § 6

# Use of medical documentation in the process of scientific research

1. The administrator of personal data contained in medical records is the medical entity, which determines the rules for the security of personal data in this respect, in particular the rules for sharing them.
2. In accordance with art. 26 sec. 4 and 5 of the law of 6 November 2008 about the patient's rights   
   and the Patient Ombudsman (i.e. Journal Journal of Laws 2020 pos. 849 as amended) medical records may be shared for scientific purposes without disclosing the name and other data enabling identification of the person to whom the records relate. Processing of personally identifiable data is only permitted by persons (students of scientific clubs and doctoral schools) are obliged to keep medical confidentiality, if the patient has not objected to contact with students at the treatment unit in connection with the provided health service.
3. The application for access to medical records for scientific purposes shall be signed by the head of the University's organisational unit in charge of the scientific research.
4. In the case of students (who are obliged to keep medical confidentiality), access to medical documentation is made at the request of the Dean after obtaining the approval of the head of the unit.
5. The method and scope of access shall be decided by the managing authority.
6. In the case of placement of an organizational unit of the University conducting scientific research on the territory of the medical entity and simultaneous employment of the researcher   
   in both of these entities at the same time, the Researcher applies the principles of sharing medical records for scientific purposes in accordance with the principles specified   
   in this regulation and adheres to the rules specified by the medical entity.

# § 7

The Order shall enter into force on the date of signing.

**Rector**

**prof. dr hab. Adam Krętowski**