Appendix no to the Main Agreement

AGREEMENT ON JOINT MANAGEMENT OF PERSONAL DATA

concluded in Białystok on ..................

by and between:

Medical University of Białystok with the seat in Białystok, Kilińskiego 1, 15-089 Białystok, represented by ..........................................................................................

hereinafter referred to as the Co-Data Controller 1

and

............................................................................................................................................................., represented by .......................................................................................................

hereinafter referred to as the Co-Data Controller 2

collectively referred to as “Co-Data Controllers” or “Parties”

Considering that the Parties jointly agree on the purposes and modalities of data processing in connection with the joint implementation of the Main Agreement No..................................... of .................., the subject of which is the implementation of scientific research between the Parties, on the basis of joint management within the meaning of Article 26 of 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 (hereinafter referred to as GDPR),

The parties have agreed to conclude a Co-Management Agreement worded as follows:

§ 1 Description of joint management

1. Under the terms of this Agreement, the Parties shall define the respective scope of their responsibility regarding the fulfilment of their obligations under the GDPR.
2. The common purpose of the processing is to carry out scientific research in the scope of ..........................
3. The purpose and manner of processing of personal data by the Co-Data Controllers arises from the Main Agreement.
4. Data categories: research participants.
5. Type of data:

-data which is de-identified insofar as possible in order to ensure as far as possible that, without access to an identifier, a person cannot be identified (pseudonymised data)

-ordinary data - name, surname, PESEL, address

-special categories of data - health data, genetic data, biological samples

1. In particular, the Parties have agreed that data will be processed, depending on the tasks they perform, as follows: PLEASE ENTER THE RESPONSIBILITIES OF THE PARTIES BELOW

Co-Data Controller 1:

* obtain approval from the relevant bioethics committee to conduct the study,
* will recruit research participants,
* obtain clinical data and pseudonymise them,

- Co-Data Controller 2:

* will participate in the preparation of joint scientific publications;

*Personal data of research participants will be pseudonymised for data protection purposes.* Co-Data Controller 1 shall transfer pseudonymised data to Co-Data Controller 2. Co-Data Controller 2 will not be able to reverse the pseudonymisation itself and identify data subjects and will not make any attempt to reverse the pseudonymisation on the data.

 **§ 2 Responsibilities of Co-Data Controllers**

1. Obligations towards data subjects involving co-processing, i.e., the obligation to provide information and the exercise of individual rights, will be carried out by Co-Data Controller 1*.* If a person subject to co-processing makes a request to Co-Data Controller 2, Co-Data Controller 2 will forward the request immediately to Co-Data Controller 1.
2. The Parties agree on the role and scope in implementing their obligations under the GDPR in this manner:
3. The Co-Data Controllers declare that they process personal data in accordance with the principles set out in Article 5 of the GDPR.
4. Co-Data Controller 1 shall keep all records relating to the co-administration, for the purpose of meeting the accountability requirement.
5. The Co-Data Controllers do not transfer personal data outside the EU and EEA.
6. When planning to make changes to the way personal data is processed, the Parties are required to comply with the privacy design requirement of Article 25(1) of the GDPR and are required to inform the Parties in advance of the planned changes in such a manner and within such timeframes as to ensure that the Parties have a realistic opportunity to react if the changes planned by a Party, in the opinion of at least one of the Parties, threaten the agreed level of security of personal data or increase the risk of a breach of the rights or freedoms of persons as a result of the processing of personal data by the Party planning the change.
7. The Parties undertake to limit access to personal data to only those persons whose access to personal data is necessary for the performance of the Agreement.
8. Personal data may only be processed by persons who have a personal authorisation granted by the Co-Data Controller and who have undertaken an obligation to keep personal data confidential.
9. Each Co-Data Controller undertakes to maintain documentation describing how personal data is processed, including a Register of Data Processing Activities.
10. Each of the Co-Data Controller shall ensure the protection of personal data and shall take measures to protect personal data as referred to in Article 32 of the GDPR in accordance with the further provisions of the Agreement.
11. Each of the Co-Data Controllers has appointed its own Data Protection Officer. The Parties have provided each other with the details of the DPO.
12. The Co-Data Controllers shall ensure that persons authorised to process personal data have received prior training on the principles and rules on personal data protection and on the consequences of violating them, including in particular the procedure for safeguarding personal data and their roles in this respect.
13. The Parties agree that in the event of a personal data breach, Co-Data Controller 1 is responsible for reporting the breach to the supervisory authority. The Parties undertake to cooperate in fulfilling their obligations in connection with a personal data breach, as further provided for in the Agreement.
14. If a personal data breach is likely to result in a high risk of infringement of the rights or freedoms of natural persons, the Co-Data Controller 1 responsible for notifying the breach to the supervisory authority shall, without undue delay, notify the data subject of such breach. The Parties undertake to cooperate in fulfilling their obligations in connection with a personal data breach, as further provided for in the Agreement.

**§ 3 Entrustment of processing**

Each Party may entrust the processing of Personal Data to another Processor by means of a written Personal Data Processing Entrustment Agreement. In such a situation, the Entrusting Party is obliged to ensure that the obligations related to the entrustment of the processing of Personal Data under the GDPR are fulfilled and to inform the Parties of the identity of the Processor.

**§ 4 Security of personal data**

1. Each of the Co-Data Controllers has carried out its own risk analysis of the processing of Personal Data and shall follow the results of that analysis as to the organisational and technical measures for the protection of Personal Data corresponding to the identified risk of infringement of the rights and freedoms of the Data Subjects. The Parties shall update their risk analysis of the processing of Personal Data according to the needs and requirements of the GDPR and inform the other Parties of the results of the update.
2. The Parties confirm that the level of protection of personal data applied by each Party corresponds to the risks identified as a result of the risk analysis referred to in the previous paragraph. In particular, each Party has assessed, informed, and undertakes to keep informed of the relevance and application of the technical and organisational measures to protect personal data.
3. Where a planned type of processing of personal data under joint control - in particular using new technologies - is, due to its nature, scope, context and objectives, likely to result in a high risk of harming the rights or freedoms of natural persons, the Parties shall in each case agree on the modalities of co-operation in assessing the effects of the planned processing operations on the protection of personal data.

**§ 5 Response times**

1. The Parties shall ensure that within 48 hours of notification of a suspected personal data breach, if the likelihood of the breach is high, the Parties notify each other of the suspected breach, allowing the Parties to participate in the investigation. Separately, the Parties shall inform each other of the determination or exclusion of a breach within 4 hours of such determination.
2. Notification of the breach to the supervisory authority shall be made by the Co-Data Controller 1. If the data breach relates to the Party which identified it, that Party shall draft the content of the notification without delay. Each Party shall maintain a log of identified personal data breaches occurring under joint controllership.
3. Each Co-Data Controller shall notify the Parties within 48 hours of any request for personal data to a competent authority of a State, unless the prohibition of notification is based on law, in particular criminal procedural law or law relating to the prevention of terrorism or money laundering.
4. Each Co-Data Controller shall notify the Parties within 48 hours of any request received to exercise a Unit Right. Where Co-Data Controller 2 notifies Co-Data Controller 1, it shall send all necessary documentation regarding the exercise of the Unit Right to allow Co-Data Controller 1 to exercise the Unit Right.

**§ 6 Contact persons**

**Contact details of the Co-Data Controllers’ DPO.**

*The DPO appointed by Co-Data Controller 1 - e-mail:* *iod@umb.edu.pl*

*The DPO appointed by Co-Data Controller 2 - e-mail:* *................................*

**§ 7 Liability**

Each of the Co-Data Controller is subject to the remedies and sanctions set out in Articles 77 - 79 and Articles 82 - 84 of the GDPR (joint and several liability). In mutual settlements, the Parties shall use the principle of fault. However, if no fault can be attributed to either Party or the degree of fault is similar, the division of liability will be made in equal parts.

**§ 8 Contract Period**

1. The agreement is concluded for the duration of the main agreement.
2. The Agreement may be terminated in accordance with the rules for termination of the main agreement, i.e., by either Party, in writing, giving 90 days' ‑notice, commencing on the date of delivery of the letter to the other Party.

**§ 9 Final provisions**

1. Annexes. The Agreement has the following annexes:

*Appendix 1 - Information on the main content of the Co-Data Controller arrangement including information on processing of personal data*

1. The Agreement shall enter into force on the date of its signature by the Parties.
2. Any amendments or additions to the Agreement shall be made in documentary form, otherwise being null and void.
3. The competent court for disputes arising in connection with the performance of the Agreement shall be the court having jurisdiction over the registered office of the Co-Data Controller 1.
4. One copy of the Agreement has been drawn up for each Party.
5. The Agreement is subject to the GDPR and Polish law, including in particular the provisions of the Civil Code.

**signatures:**

**Appendix 1 Information on the main content of the Co-Data Controller arrangement including information on processing of personal data**

In accordance with Article 13 or 14 and Article 26 of 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) (hereinafter referred to as GDPR), we inform you about the fact that we jointly process your personal data and inform you about the essential content of the joint arrangements of the Co-Data Controller.

1. The Co-Data Controllers of your personal data are:
* Medical University of Białystok - ul. Jana Kilińskiego 1, 15-089 Białystok, (hereinafter referred to as "Co-Data Controller 1")
* **......................................................................................................** (hereinafter “Co-Data Controller 2”)
1. The Co-Data Controllers jointly administer your personal data for the purpose of jointly carrying out research as part of a scientific project entitled “........................................................”.
2. Your data will be processed on the basis:

- Article 6(1)(a) of the GDPR and Article 9(2)(a) - consent to data processing,

- Article 9(2)(j) GDPR - processing is necessary for the purposes of scientific research under the Higher Education and Science Act,

1. The recipients of your personal data may be entities entrusted by the Co-Data Controllers to process the data, including, IT service providers.
2. We plan to keep your data for the period necessary to carry out the project or until you withdraw your consent.
3. You have the right to access your personal data, to request rectification of your personal data, erasure, restriction of processing of your personal data, the right to data portability - under the terms of the GDPR.
4. To the extent that the processing of your personal data is based on consent, you have the right to withdraw your consent without affecting the compatibility of the processing previously carried out.
5. No automated decisions will be taken on the basis of the personal data provided, including no profiling.
6. You have the right to lodge a complaint to the supervisory authority, which is the President of the Personal Data Protection Office, Stawki 2, 00-193 Warsaw.
7. The data is provided voluntarily
8. In connection with the processing of your personal data we also inform you that:
* The Co-Data Controllers declare that they process your personal data in accordance with the principles relating to the processing of personal data set out in Article 5 of the GDPR.
* Co-Data Controller 1 shall keep accumulated records of

joint management, for the purposes of meeting the accountability requirement.

* The Co-Data Controllers shall not transfer your personal data outside the EU and EEA.
* The Co-Data Controllers undertake to restrict access to your personal data to only those persons whose access to the personal data is necessary for the purposes mentioned above. In addition, the Co-Data Controllers shall ensure that only persons who have a personal authorisation granted by the Data Controller are allowed to process personal data, and that persons allowed to process personal data have taken an undertaking to keep personal data confidential, and that persons have been previously trained in the principles and regulations of personal data protection.
* The Co-Data Controllers shall ensure an adequate level of security of personal data.
1. The Co-Data Controllers, in the interests of security, ensure that you can contact the Co-Data Controllers on all matters relating to the protection of your personal data, but it is Co-Data Controller 1 who will write to you and see that your rights are exercised. This means that ideally you should direct communications regarding the exercise of your rights to: Co-Data Controller 1’s Data Protection Officer, by email to iod@umb.edu.pl