Appendix No ... to the Main Agreement

Personal Data Processing Entrustment Agreement,

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

by and between:

Medical University of Bialystok, Kilińskiego 1, 15 – 089 Białystok, hereinafter referred to as the “Data Controller” represented by .....................................................................

and

................................................ hereinafter referred to as “Processor” represented by ..............................................

Whereas:

- The parties have entered into the Agreement No. ..................................... of .................. on the subject of ................................... hereinafter referred to as the Main Agreement.

- The execution of the Main Agreement requires the Data Controller to entrust the processing of personal data to a Processor, within the meaning of Article 28 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 the repeal of Directive 95/46/EC (hereinafter referred to as GDPR),

The Parties have decided to conclude a Personal Data Processing Entrustment Agreement worded as follows:

Due to the fact that the outsourcing of the processing of personal data takes place to a Processor who is a third country in accordance with the GDPR, the Data Controller entrusts the processing of personal data to the Processor on the basis of a European Commission adequacy decision in accordance with Chapter V of the GDPR .

§1

Subject, scope and purpose of data processing

1. The subject matter of the agreement is the entrustment of personal data for processing by the Data Controller to the Processor, pursuant to Article 28 of the General Data Protection Regulation of 27 April 2016.
2. (hereinafter referred to as GDPR) on the terms and for the purpose specified in this Agreement. The Processor undertakes to process the personal data entrusted by the Data Controller solely for the purpose of *implementing the* Main Agreement.
3. Categories of data subjects: research participants
4. Data categories: pseudo-anonymised data / ordinary data / detailed data\*(please select as appropriate), including: .............................................................................................................................................

-data which is de-identified to the greatest extent possible to ensure that, without access to an identifier, it is impossible to identify a person - code

-ordinary data - name, surname, PESEL, address

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

1. The following processing activities may be carried out on the entrusted personal data resulting from the subject matter of the main contract, which concerns the performance of analysis of biological samples, performance of DNA sequencing, performance of research\* (*please select or enter as appropriate*): collection, transmission, editing, copying, destruction, storage, organisation, viewing/analysing\* (*please select or enter as appropriate*)

The Processor will not be able to reverse the pseudonymisation itself and identify data subjects and will not carry out any attempt to reverse the pseudonymisation on the entrusted data .

§2

Obligations of the Processor

1. When processing the personal data entrusted to it, the Processor shall undertake to secure the personal data by applying appropriate technical and organisational measures which ensure an adequate level of security corresponding to the risks involved in the processing of personal data, as referred to in Article 32 of the GDPR.
2. The Processor shall exercise due diligence in processing the entrusted personal data.
3. The Processor declares that access to the processing of personal data will be granted only to authorised persons who will process the entrusted data solely for the purpose of implementing this agreement.
4. The Processor undertakes to ensure that the processed data and the means of securing the data are kept confidential by the persons who will have access to the data, both during and after their employment with the Processor.
5. The Processor declares that in connection with the obligation to keep the
data confidential, the data shall not be used, disclosed or made available without the written consent of the Data Controller for any purpose other than the performance of the agreement, unless the necessity to disclose the information held results from applicable law.
6. The Processor undertakes to protect the entrusted data against unauthorised or unlawful processing (destruction, loss, modification, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise processed) by means of appropriate technical or organisational measures.
7. The Processor undertakes to assist the Data Controller to the
necessary extent in fulfilling the obligations to respond to requests from the data subject and to comply with the obligations set out in Articles 32 to 36 of the GDPR.

§3

Reporting of infringements

1. The Processor undertakes, upon discovery of a personal data breach, to notify it to the Data Controller without undue delay and no later than within 24 hours.
2. The information provided to the Data Controller should include at least:
3. a description of the nature of the breach and, where possible, an indication of the category and approximate number of data subjects affected and the amount/type of data affected,
4. a description of the possible consequences of the breach,
5. a description of the measures applied or proposed to be applied by the Processor to remedy the breach, including minimising its adverse effects.

§4

Right of control

1. The Data Controller pursuant to Article 28(3)(h) of the GDPR has the right to control whether the measures applied by the Processor in processing and securing the entrusted personal data meet the provisions of the agreement.
2. The Data Controller shall exercise the right of inspection during the business hours of the Processor and with a minimum of 7 days’ notice.
3. The Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and allow the Data Controller or an auditor authorised by the Data Controller to carry out audits.
4. The Processor shall be obliged to remove the deficiencies found during the audit within the time limit indicated by the Data Controller, not exceeding 14 days, unless the removal of the deficiencies within this deadline is not possible, the Processor may agree a different deadline.

§5

Further entrustment of data processing

1. The Processor may entrust the personal data covered by this agreement to subcontractors for further processing only for the purposes of performing the agreement after obtaining the prior written consent of the Data Controller. Written consent shall also mean consent sent by email.
2. The subcontractor referred to in §5.1 of the agreement shall meet the same guarantees and obligations as those imposed on the Processor in this agreement.
3. The Processor shall be fully liable to the Data Controller for any failure to fulfil the subcontractor's data protection obligations.

§ 6

Responsibility of the Processor

1. The Processor shall bear the responsibility for sharing or using personal data in violation of the Agreement, in particular for disclosing the personal data to unauthorized parties.
2. The Processor undertakes to inform the Data Controller without delay of any proceedings, in particular administrative or judicial, relating to the processing of personal data entrusted by the Data Controller specified in the agreement, of any administrative decision or ruling concerning the processing of such data, addressed to the Processor, as well as of any planned, if known, or carried out checks and inspections regarding the processing of such personal data at the Processor.

§7

Duration, termination of the Agreement

1. This Agreement shall apply from the date of its conclusion for the duration of the Main Agreement.
2. The Data Controller may terminate this Agreement with immediate effect when the Processor:
3. despite being obliged to remedy the shortcomings found during the inspection, fails to do so within the time limit set;
4. processes personal data in a way incompatible with the agreement;
5. entrusted the processing of personal data to another entity without the consent of the Data Controller.
6. The Processor shall be entitled to carry out the processing of personal data only until the expiry or termination of the agreement, taking into account paragraph 4.
7. Within 14 days after the termination of the Agreement, the Processor shall be obliged, *\*to remove or to return (\*select as appropriate)* the entrusted personal data from all media, programs, applications, including copies, results of analyses and research, and other data which were generated during the processing of the entrusted personal data, unless the obligation of their further processing results from separate provisions of law.

§8

Final provisions

1. The Agreement has been drawn up in two identical copies for each party.
2. In matters not regulated, the provisions of generally applicable law, including the GDPR shall apply.
3. Amendments to the Agreement shall be made in writing under pain of nullity.

Data Controller Processor