**Data Processing Agreement**

between:

The University of Warmia and Mazury in Olsztyn, Oczapowskiego 2, 10-719 Olsztyn, Poland (henceforth referred to as the “**Controller**”), represented by:

………………………………………………………………………

and

……………………………………………………………………..

(information about the second party to the Agreement), henceforth referred to as the “**Processor**”, represented by:

………………………………………………………………………

Date: …………………. Olsztyn

**§ 1**

**Outsourcing of personal data processing**

1. The Controller transfers the data to the Processor for processing under the terms and conditions laid down in this Agreement, in compliance with Article 28 of the Regulation 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 (henceforth referred to as “**GDPR**”.)
2. The Controller hereby declares that it is the controller of the data which is transferred to the Processor for processing.
3. The Processor undertakes to process personal data on behalf of the Controller in accordance with the conditions laid down in this Data Processing Agreement, GDPR and other provisions of law in force regarding the protection of rights of data subjects.

**§2**

**Purpose and scope of data processing**

1. Under the terms and conditions laid down in this Agreement, the Processor shall process the data transferred by the Controller for processing:……………….. (the type of data must be provided, e.g. common data or special categories of data, the category of data subjects and what kind of data is transferred, e.g. names, PESEL [personal identification number] etc.)
2. The Processor shall only process the data transferred by the Controller for:……………..(the purpose of data processing must be provided, e.g. completing the services laid down in Consent no. ………, dated……..).

**§ 3**

**Processor’s Obligations**

1. For the processing of the data transferred by the Controller, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR.
2. The Processor shall exercise due diligence in order to ensure the proper processing of personal data.
3. The Processor shall grant proper authorizations for data processing to every person who participates in processing the data transferred for processing by the Controller under the terms and conditions laid down in this Agreement.
4. The Processor shall treat all the Personal Data as strictly confidential information (complying with Article 28 para 3 (b)) and ensure that its employees and other representatives accessing the data, who will receive proper authorizations for data processing under the terms and conditions laid out in this Agreement, are bound by a commitment of confidentiality during the time they are employed by the Processor and after the termination of their employment contract.
5. The Processor shall delete or return the data to the Controller after the completion of services laid out in the contract. The Processor shall also ensure the destruction of all existing copies, unless EU regulations or the law of a member state law requires to retain the data.
6. Parties to the Agreement shall assist each other in ensuring compliance with the obligations laid down in this Agreement, especially regarding the cooperation between the Parties in case of a data subject exercising their right of access to their data which is being processed, and ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR
7. The Processor shall immediately contact The Controller - within 24 hours - if there is any personal data breach or incident where the Data may have been compromised.

**§ 4**

**Audit**

1. The Controller shall be at liberty to conduct an audit for the Processor to demonstrate whether the security measures are in compliance with § 3 (1) of this DPA and statutory conditions. The Controller shall inform the Processor about exercising its right to carry out an audit with a prior written notice, which is to be received by the Processor no later than 3 days before an audit. After receiving the notification, the Processor may submit a request for the Controller to carry out the audit at an earlier date.
2. For an audit to be carried out in compliance with (1) of this article, the Controller shall make reasonable endeavors to avoid causing damage or disruption to the Processor’s premises (taking into consideration working hours of the Processor) in the course of such an audit.
3. During an audit, the Processor shall make available to the Controller all relevant information necessary to assess the adequacy of applied security measures appropriate to the risk, especially paper records and databases.
4. The Processor shall implement corrective action to remedy any deficiencies identified during the audit and described in the post-audit report. These deficiencies are to be corrected no later than 7 days after the completion of the audit and the presentation of the post-audit report by the Controller.

**§ 5**

**Sub-contracting of processing**

1. The Processor is given authorization to engage third-parties to process the data transferred under this Agreement (“Sub-Processors”) after obtaining written, specific authorization from the Controller.
2. The Agreement to engage Sub-Processors shall be concluded only to execute this Agreement and shall regard only the data transferred and specified in this Agreement – their type, scope and purpose of processing.
3. The data can be transferred to a third country only after a written instruction issued by the Controller, unless the Processor is bound by such obligation by the law of the European Union or one of its member states to which the Processor is subject. In that case, the Processor shall inform the Controller about such obligation before processing the data, unless the law prohibits passing forward such information because of important public interest.
4. The Sub-Processor shall fulfill the same guarantees and obligations as the Processor under this Agreement, and shall guarantee the proper execution of its obligations regarding the security of personal data.
5. The Processor is fully accountable to the Controller for any action of the Sub-Processor not complying to the provisions of the Agreement regarding the protection of data.

**§ 6**

**Responsibilities of the Processor**

1. The Processor shall be held accountable for the use of personal data contrary to the provisions of this Agreement, including in particular for the disclosure of data transferred by the Controller to the unauthorized third-parties.
2. The Processor shall, without delay, inform the Controller about any proceedings, in particular court or administrative ones, regarding data processing by the Processor as a result of this Agreement, and shall inform the Controller about any administrative decision or ruling regarding processing of this data, as well as any audit and inspection regarding personal data processing as a result of this Agreement, in particular these carried out by the officials authorized by the President of the Personal Data Protection Office.
3. In the case of a third party taking legal action against the Processor and/or the Controller regarding the violation of GDPR, the Processor shall assist the Controller to take appropriate legal steps aimed in particular at the dismissal or rejection of the claim of the third party by the competent court, bringing an appeal or settlement, as well as taking other legal action.

**§ 7**

**Duration of the Agreement**

1. This Data Processing Agreement comes into force from the day of its conclusion for indeterminate duration/for a fixed period from…. to…./for the duration of general Agreement no. …………..
2. Either Party may, by giving one month’s written notice to the other Party, terminate this Agreement/and general Agreement no. ............... dated ................ within its designated timeframe.
3. The Controller shall terminate this Agreement and general Agreement no. ....... dated ....... with immediate effect in case of the Processor:
4. failing to implement corrective action to remedy the deficiencies identified during an audit referred to in § 4 of this Agreement within the prescribed time limit,
5. processing the personal data contrary to the conditions laid down in this Agreement,
6. engaged a third-party to process the personal data without obtaining authorization from the Controller.

**§ 8**

**Confidentiality rules**

1. The Processor undertakes to keep confidential all information, data, materials, documents and personal data received as a result of this agreement from the Controller and other parties associated with the Controller, or information the Processor has received in its role as Processor (henceforth referred to as “**Confidential Information”**).
2. The Processor shall not use, disclose or share Confidential Information for any purposes other than for the purposes of this Agreement without obtaining written authorization from the Controller, unless the disclosure of information in the Processor's possession is required by applicable laws and by this Agreement.
3. Parties to this Agreement shall exercise due diligence in order to ensure that the means of communication used to receive, transfer and store the Confidential Information guarantee its security, including, in particular, protection which prevents access by unauthorized third parties to personal data transferred for processing.

**§ 9**

**Miscellaneous**

1. The Agreement is drawn up in duplicate, one for each party.
2. Relevant provisions of the Polish Civil Code and GDPR shall apply for matters not covered by this Agreement.
3. Any dispute arising between the Parties in connection with and/or arising from this Data Processing Agreement will be referred to the competent court in the district where the Controller has its seat.