Detailed rules on joint processing, data processing and data transfers

The **University of Óbuda** (hereinafter referred to as "**University**") is subject to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council 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 "**Regulation**" or "**GDPR**") and the provisions of the Act on the right to information self-determination and freedom of information of 2011. CXII of 2011 (hereinafter referred to as the „**Data Protection Act**" or „**Infotv.**"), and in order to regulate data protection and data security with regard to the principle of accountability set out in Article 5(2) of the Regulation, the following details the issues arising in connection with the joint processing, processing and transfer of data involving the University.

This document forms an integral part of the University's Data Protection and Privacy Policy.

1. Shared data management

1.1. Where the University determines the purposes and means of processing for which it is responsible jointly with another University (hereinafter jointly referred to as "**joint controllers**"), it shall be considered joint processing. Joint controllers shall, before joint processing commences, enter into an agreement setting out the division of responsibilities for the performance of their tasks in relation to the obligations imposed by data protection legislation, unless the division of responsibilities is provided for by law.

1.2. The agreement sets out the obligations and responsibilities of the joint controllers vis-à-vis the data subjects and how to communicate with them. The most important aspects of joint processing shall be communicated to the data subject as set out in the agreement.

1.3. The data subject may exercise his or her rights under this Regulation in relation to and against each controller. The joint controllers shall cooperate to ensure the rights.

2. The data processor

2.1. If a natural or legal person carries out any data processing operation in the course of its activities on behalf of and on behalf of another person, the data processor shall be considered a data processor within the meaning of Article 4(8) of the Regulation in respect of the operation(s) and the data transferred, and shall carry out data processing within the meaning of Article 3(17) of the Data Protection Act.

2.2. **Commissioning of a data processor by the University**

The University shall enter into a data processing contract with the natural or legal person who processes personal data on behalf of the University, on the basis of the mandate and instructions of the University, with the content of Article 28 of the Regulation. The processor shall act only on the basis of written instructions from the University and shall not take any substantive decisions regarding the processing of personal data. If a processor goes beyond the scope of the mandate, in particular if it processes data for purposes other than those for which it was mandated (including its own), it becomes an independent controller in respect of that overlap.

The data processing contract shall clarify at least the following issues:

a) the processing purposes for which the University uses the services of the data processor;
b) the processing activity performed by the processor;
c) the duration, nature and purpose of the processing;
d) the type of data transferred for processing;
e) the categories of data subjects concerned by the processing;
f) the rights and obligations of the controller;
g) the rights and obligations of the data processor.

The University will only enter into a contract with a data processor for data processing tasks where the data processor agrees in the contract to:

a) process personal data only on the basis of written instructions from the University;
b) ensures that the persons involved in the processing of personal data by it are bound by an obligation of confidentiality or are under an appropriate obligation of confidentiality based on law;
c) take data security measures in accordance with Article 32 of the Regulation.
d) will not use any other processor without the prior written authorisation of the University, whether general or ad hoc;
e) assist the University, to the extent possible and taking into account the nature of the processing, by appropriate technical and organisational measures, in fulfilling its obligation to respond to requests relating to the exercise of the rights of data subjects;
f) in the event of a personal data breach, notify the University without delay as soon as it becomes aware of the personal data breach and cooperate in the handling of the personal data breach;
g) delete or return to the University, at the University's discretion, all personal data and destroy or delete copies of personal data at the same time after the processing service has been completed;
h) enables and facilitates the University to monitor compliance with data protection rules;
i) keep the register of data processors referred to in Article 30(2) of the Regulation.

The contract for the processing of data must be in writing.

Prior to the start of processing, the University shall make sure that the processor has taken the necessary technical and organisational measures to ensure an adequate level of data protection in its day-to-day activities.

The rights and obligations of the data processor in relation to the processing of personal data shall be determined by the Rector. The Rector or a person designated by him shall have the right to instruct the processor on behalf of the University. The person employed by the University who has the right to give instructions shall be responsible for the lawfulness of the instructions given.

The processing should not be entrusted to an organisation that has an interest in the business of using personal data.

2.3. **Data processing activities carried out by the University**

If the University carries out any data processing activity on behalf of another (legal) person in the course of its activities, the University shall be considered a data processor within the

meaning of Article 4(8) of the Regulation in respect of the entrusted operation(s), and shall carry out data processing within the meaning of Article 3(17) of the Data Protection Act.

With regard to the fact of data processing, the University shall enter into a data processing contract with the client as referred to in Section 2.2.

The client shall have the right and the obligation to give the University written instructions regarding the processing of data. The client shall be responsible for the lawfulness of the instruction. The University may only carry out its processing activities on the basis of this instruction, and may not take any substantive decisions regarding the processing, nor may the University determine the purposes for which the data are processed or use the data for any other purpose.

3. Data transmission

3.1. A transfer is the making available of personal data to a specified third party. A third party is any person or organisation other than the University, the data subject and any processor that is an independent controller and does not fulfil the conditions for joint processing.

3.2. The University shall verify, prior to the transfer of the personal data it is processing, whether the conditions for the transfer of the personal data are met, in particular whether it is a controller of the data requested, whether it has a legal basis for the transfer of the data and whether the transfer complies with the purpose limitation principle.

3.3. It is the responsibility of the employee carrying out the transfer to check that the conditions for the transfer are met. The transfer of data for processing does not constitute a transfer within the meaning of the above.

3.4. Except in the case of mandatory data transfer, the Rector is responsible for the processing of data transfer requests submitted by third parties. A request for transfer may be granted if it contains:

a) the data necessary to identify the data subject beyond reasonable doubt;
b) the purpose of the transfer, the legal basis for the transfer (specifying the legal provision on which the transfer is based);
c) the exact scope of the data requested;
d) the data necessary to identify the person concerned.

3.5. If the transfer cannot be lawfully carried out or if the information necessary for the assessment of the request has not been provided by the applicant after the request, the transfer shall be refused. The refusal to transfer, together with the reasons for it, shall be notified in writing to the applicant.

3.6. The transfer of data may be made on the basis of an individual request or, by law or by agreement, by direct access.

4. Data transfers to third countries

4.1. Transfers of personal data, including retransfers of personal data from a third country to another third country, which are or are intended to be subject to processing following their

transfer to a third country or an international organisation, may only take place if the University complies with, inter alia, the following conditions set out in Chapter V of the Regulation.

4.2. Transmission of data under a conformity decision

The University first checks whether the European Commission has issued a conformity decision for the country concerned. A transfer of personal data to a third country may take place without further authorisation if the Commission has determined that the third country, a territory or one or more specific sectors of the third country provide an adequate level of protection.

4.3. Data transmission with appropriate guarantees

Where there is no adequacy decision, the data may be transferred if the University provides adequate safeguards and the data subjects have enforceable rights and effective remedies.

Without specific authorisation from the supervisory authority, appropriate guarantees may include:

a) a legally binding and enforceable instrument between public authorities or other bodies with a public-service mission;
b) binding corporate rules;
c) general data protection clauses adopted in accordance with the examination procedure;
d) an approved Code of Conduct, together with a binding and enforceable commitment by the third country controller or processor to apply appropriate safeguards, including on data subjects' rights;
e) an approved certification mechanism, together with a binding and enforceable commitment by the third country controller or processor to apply appropriate safeguards, including with respect to the rights of data subjects.

The University transfers personal data in the case referred to in point (c) above, both between data controllers and between data controllers and data processors, using one of the model contracts specified by the authorized body of the European Union.

For international data transfers to entities within a group of undertakings or the same group of undertakings engaged in joint economic activities, it is possible to apply binding corporate rules approved by the public authority, which provide an adequate guarantee for the transfer as referred to in point (b) above.

In particular, the following may also serve as appropriate safeguards, subject to the supervisory authority's approval:

a) contractual arrangements between a controller or processor and a controller, processor or recipient of personal data in a third country or within an international organisation; or
b) provisions between public authorities or other bodies with a public-service mission to be incorporated into an administrative agreement, including provisions on the enforceable and effective rights of data subjects.

4.4. Derogations granted in a specific situation

In the absence of a decision of adequacy or appropriate safeguards, the transfer or multiple transfers of personal data to a third country or international organisation may only take place if at least one of the following conditions is met:

a) the data subject has given his or her explicit consent to the envisaged transfer after having been informed of the potential risks of the transfer due to the lack of a conformity decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the data subject;
c) the transfer is necessary for entering into, or performance of, a contract between the controller and another natural or legal person which is in the interest of the data subject;
d) the transfer is necessary for important public interests;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary for the protection of the vital interests of the data subject or of another person and the data subject is physically or legally incapable of giving consent;
g) the data transmitted originate from a register which serves the purpose of informing the public within the meaning of Union or Member State law and which is accessible for consultation by the public in general or by any person having a legitimate interest therein, but only if the conditions for consultation laid down by Union or Member State law are fulfilled in the specific case.