Data Management and Privacy Policy

UNIVERSITY OF ÓBUDA

Budapest, 2022.

(In force from 1 December 2022)

Content

Preambulum

The **University of Óbuda** (hereinafter: "**University**", "**Controller**") is a higher education institution maintained by a foundation, a legal entity operating on the basis of the rights granted by the National Higher Education Act.

The 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 "the **Regulation**" or „**GDPR**") and the provisions of Act CXII of 2011 on the right to information self-determination and freedom of information. (hereinafter referred to as the "**Infotv.**"), to regulate its internal data management processes, to keep records thereof and to ensure the rights of data subjects, to regulate data protection and data security, and with regard to Article 24 of the Regulation, the following Data Protection Policy (hereinafter referred to as the "**Data Protection Policy**", "**Policy**") is hereby adopted.

Name of data controller:	**University of Óbuda**
Institutional identification number:	**FI12904**
Data Controller's registered office:	**1034 Budapest, Bécsi út 96/B**
E-mail address of the controller:	**jog@uni-obuda.hu**
Representative of the Data Controller:	**Prof. Dr. Levente Kovács Rector**
Data Protection Officer:	**Bovard Kft. (info@bovard.hu)**

Chapter I

GENERAL PROVISIONS

1. Purpose of the Policy

1.1. The purpose of this Policy is for the University to define the rules governing the handling, transmission, processing and protection of personal data processed in the context of its operations, the roles and responsibilities of the departments and persons involved in the processing of personal data, and the responsibilities for the processing of personal data.

2. Scope of the Policy

2.1. The scope of this Policy applies to persons employed by the University and persons employed by the University in other employment relationships (hereinafter collectively referred to as "**Employee(s)**").

2.2. The scope of the Policy covers all processes involving the processing of personal data at the University, regardless of the processing method, and personal data held by the University.

2.3. This Policy and the provisions contained herein shall enter into force on 1 December 2022, following approval by the Senate.

2.4. The provisions of this Policy shall be interpreted in accordance with the provisions of other University policies. In the event of a conflict between the provisions of this Policy and the

provisions of other University policies with respect to the processing or protection of personal data, the provisions of this Policy shall apply.

3. Concepts

3.1. The conceptual system of the Rules corresponds to the conceptual system defined in Article 4 of the Regulation and Article 3 of the Infotv.

3.2. Where the definitions in the applicable data protection legislation differ from the definitions in the Policy, the definitions in the legislation shall prevail.

3.3. Where the Policy or any other University document governing the processing of personal data refers to data processing or data, it shall be understood to mean the processing of personal data or personal data, unless otherwise stated.

4. Principles of data management and the tasks to be carried out in order to comply with them

4.1. Purpose limitation of data processing

4.1.1. Personal data may be processed only for specified, explicit and legitimate purposes and on one of the legal bases set out in the Regulation .

4.1.2. Personal data processed for a specific purpose will be processed by the University for purposes other than those for which they were originally collected only if there is an appropriate legal basis. The University is obliged to duly inform the data subject of the processing for a purpose other than the original purpose before further processing.

4.1.3. The University shall ensure that access to personal data is restricted to those employees or data processors whose processing is subject to the purpose limitation principle.

4.1.4. The Rector is responsible for ensuring the implementation of the principle of purpose in the organisation of the University.

4.1.5. When the processing starts, the University defines the purpose of the processing. Once the purpose has been achieved, the personal data processed will be deleted. The University shall not delete the data if the processing is carried out for other purposes in the interests of the University or if the storage of the data is necessary for the exercise of the rights of the data subjects.

4.2. Lawful, fair and transparent processing

4.2.1. The University shall inform the data subject of the essential characteristics of the processing in order to ensure the principle of transparency. The characteristics of the processing shall also be recorded in writing.

4.2.2. The University processes the data in accordance with the data protection and sectoral legislation governing data processing.

4.2.3. The University shall inform the data subject of the essential characteristics of the processing in order to ensure the principle of transparency. The characteristics of the processing shall also be recorded in writing.

4.2.4. In accordance with the principle of lawfulness, the University continuously examines in all its data processing whether the data have been processed in accordance with the applicable data protection legislation, in particular the GDPR and possibly the Infotv., and whether the appropriate legal basis for the processing exists, and whether the data are processed on the basis of the appropriate legal basis.

4.2.5. For each processing operation, the University will determine the legal basis for the processing and whether the necessary documentation supporting the legal basis for the processing is available. In particular, the legal basis for the University's processing and the necessary documentation are:

a) With regard to processing based on the data subject's consent, a documented statement by the data subject or his or her legal representative giving his or her unambiguous consent to the processing of personal data concerning him or her, either in full or in relation to specific operations;
b) With regard to processing necessary for the performance of a contract concluded or to be concluded with a data subject, the contract concluded with the data subject;
c) With regard to the processing necessary for the performance of a legal obligation to which the University is subject, the precise legal provision imposing or necessitating the processing;
d) To carry out a balancing of interests test where the University or a third party has a legitimate interest.

4.2.6. In order to document the processing based on consent, the University should review, for each processing based on consent, whether

a) Whether documentation supporting the legal basis is available and has been obtained in accordance with internal procedures;
b) Whether consent was the appropriate legal basis for processing the data;
c) Whether the consent has been obtained in the correct format;
d) Whether the data subject was duly informed before consent was given.

4.3. **Data economy**

4.3.1. The University only processes personal data that is adequate, relevant and necessary for the purposes for which it is processed. It will process personal data only to the extent and for the duration necessary to achieve its purpose.

4.3.2. The scope of personal data necessary to achieve the specific processing purposes, the time of processing and the characteristics of each processing operation are set out in the privacy notices published by the University.

4.4. **Accuracy**

4.4.1. The personal data processed by the University is accurate and up to date. The University will take all reasonable steps to ensure that personal data which are inaccurate for the purposes for which they are processed are promptly deleted or rectified.

4.4.2. The University shall periodically review the accuracy and currency of the data maintained in its records in order to fulfil its obligations under Section 4.4.1.

4.4.3. In any case, the University reminds the data subject that he or she is obliged to notify any changes to his or her personal data without delay.

4.5. **Limited shelf life**

4.5.1. Personal data are stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.5.2. The processing (storage) of data for a longer period than described in section 4.5.1 is only carried out for archiving purposes in the public interest, or for scientific and historical research or statistical purposes, or where necessary to ensure the exercise of the rights of data subjects.

4.5.3. The University determines the duration of the processing by purpose, to the extent necessary to achieve the purpose, taking into account the applicable legislation.

4.6. **Accountability**

4.6.1. The University will ensure compliance with the applicable laws in the processing of personal data in a way that can be verified ex post.

4.6.2. The University shall record in writing all relevant circumstances and actions taken in relation to the lawful processing of personal data, in particular, but not limited to, impact assessments carried out, interest assessments, the legal justification for decisions regarding the processing and the fact of the data subject's consent, in order to comply with the provisions of Section 4.6.1.

5. Data security

5.1. At all times during the processing of personal data, the University ensures the highest level of security that can reasonably be expected for the personal data processed. The University shall carry out its processing operations in such a way as to ensure adequate security of personal data and protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by implementing appropriate technical and organisational measures. In addition, the University shall take appropriate measures to protect personal data in particular against unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used. To ensure this, the University shall, inter alia, make back-up copies as set out in Section 5.9.

5.2. The University shall plan and carry out its data processing operations in such a way as to ensure the protection of the privacy of data subjects in the application of the law applicable to data processing.

5.3. The data controller or the designated department shall verify that the processed data are transferred to a controller or processor that ensures the security of the data.

5.4. The University shall implement appropriate technical and organisational measures to ensure a level of data security appropriate to the level of risk, taking into account the state of science and technology and the cost of implementation, the nature, scope, context and purposes of the processing, and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons. It shall ensure the security of the data, take the technical and organisational measures and establish the rules of procedure necessary to enforce the Regulation and other personal data protection rules.

5.5. When processing personal data, the University ensures that:

a) prevent unauthorised data entry;
b) prevent the use of data processing systems by unauthorised persons using data transmission equipment by applying a firewall.

5.6. To ensure the security of the personal data processed on paper, the University applies the following measures:

a) the data is known only to those authorised to access it and cannot be accessed or disclosed to others;
b) keep documents in a lockable room equipped with a security and fire alarm system;
c) access to active, ongoing documents under management is restricted to the authorized authorities;
d) the employee carrying out the processing leaves the premises where the processing is taking place during the day only by locking the data media entrusted to him or by closing the office;
e) the data controller locks away the paper medium used by the employee when the work is finished;
f) where personal data processed on paper are digitised, apply the security rules applicable to digitally stored documents;
g) paper documents containing personal data are destroyed in such a way that their data content cannot be restored later by any method (shredding);
h) determine in advance in the filing plan the duration of storage of paper documents and the date of their destruction, based on legal provisions or a decision taken by the University.

5.7. The University uses the following measures and safeguards to ensure the security of personal data stored on computers and networks:

a) in the course of data processing, employees primarily make use of assets that are owned by the University or over which the University has equivalent rights of ownership;
b) access to the University's IT system from outside is secure and only possible with a username and password;
c) access to the data on the computer is only possible with valid, personal, identifiable access rights - at least a user name and password - and the University regularly ensures that passwords are changed;
d) if the purpose of the processing has been achieved and the time limit for processing has expired, the data will be irretrievably deleted;
e) employees are only entitled to use the e-mail address "@uni-obuda.hu" provided by the University in connection with their work;
f) the e-mail address under point (e) may not be used by employees for private purposes;

g) the University shall provide virus protection and firewall protection on the network handling personal data; it shall prevent unauthorised persons from accessing the network by using the available computer tools.

5.8. The University will take special care to ensure the principle of data security when transferring data and will only transfer data through secure channels.

5.9. The University will ensure that in the event of a physical or technical incident, access to and availability of personal data can be restored in a timely manner through regular backups. In the event of restoration from backup, the University will ensure that deleted or corrected personal data cannot be restored.

5.10. The University will only print out electronically processed personal data where it is specifically required for the exercise of a right or the performance of an obligation.

The University implements appropriate technical and organisational measures to ensure that, by default, only personal data that is necessary for the specific purpose of the processing is processed. This obligation relates to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. These measures ensure that personal data are by default not made available to an indeterminate number of persons without the intervention of a natural person.

5.11. The University will ensure that access to different categories of personal data is restricted to persons employed in positions whose job duties relate to the processing of that personal data. Employees shall have their own password and user account for computer systems to ensure that unauthorised access is prevented. Paper files containing personal data shall be stored in such a way that only those employees who are authorised to handle personal data have access to them.

6. Legal basis for processing

6.1. The processing of personal data is lawful only if and to the extent that at least one of the following conditions is met:

a) the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract;
c) processing is necessary for compliance with an obligation under EU or national law to which the controller is subject;
d) processing is necessary for the protection of the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

6.2. Where the University processes personal data for purposes other than the purpose for which the data were collected, and the processing is not based on the consent of the data subject or on a legal provision, the University will take into account the following before starting the processing:

a) the purposes for which the personal data are collected and any links between the purposes for which further processing is envisaged;
b) the circumstances in which personal data are collected, in particular the relationship between the data subjects and the University;
c) the nature of the personal data, in particular whether special categories of personal data are processed and whether data relating to criminal liability and criminal offences are processed;
d) the possible consequences for the data subjects of the envisaged further processing of the data;
e) the existence of appropriate guarantees.

6.3. Details of the possible legal bases for the University's data processing are set out in a separate annex under Chapter VIII of the Policy.

7. Rights of persons concerned and their enforcement

7.1. Details of the rights of data subjects are set out in a separate annex under Chapter VIII of the Policy.

7.2. Data subjects may contact the University electronically, in person or by post in order to exercise their rights as detailed in a separate annex under Chapter VIII of the Policy, to request information on data processing and to make comments.

7.3. The University shall comply with requests for the exercise of the rights of the data subject in accordance with the relevant internal procedures set out in Chapter VIII of the Policy and the Regulation.

7.4. The data subject shall have the right to a judicial remedy, as detailed in a separate annex under Chapter VIII of the Policy, if he or she considers that the Controller or a processor acting on his or her behalf or at his or her instructions is processing his or her personal data in breach of the provisions of the law on the processing of personal data.

7.5. The data subject may contact the University with any questions, comments, requests or complaints regarding the processing of his or her personal data by e-mail at jog@uni-obuda.hu, by post or in person at the University's headquarters. In such a case, the University will investigate the matter within a maximum of 30 days and inform the data subject of the outcome of the investigation.

7.6. If the University does not take action on the data subject's request, it shall also inform the data subject of the authority with which he or she may lodge a complaint or seek judicial redress and under what conditions.

7.7. The data subject shall not be discriminated against for exercising the right to the processing of personal data provided for in the Policy or in any legislation.

7.8. The manner in which the rights relating to the processing of personal data may be exercised after the death of the data subject is set out in a separate annex under Chapter VIII of the Policy.

Chapter II

PARTICIPANTS TO THE PROCESSING

8. The organisation of data management

8.1. **The rector**

8.1.1. Pursuant to Article 13 (1) of Act CCIV of 2011 on National Higher Education, the rector is the primary responsible manager and representative of the institution of higher education. Accordingly, the Rector is responsible for the lawfulness of the University's data management.

The Rector's Office, which is subordinate to the Rector, assists the Rector in his/her work and duties.

8.1.2. The Rector shall define and establish internal rules and systems of internal rules on data protection, taking into account the specificities of the University.

8.1.3. The Rector on the University's data protection activities:

a) is responsible for ensuring the conditions necessary for the exercise of the rights of data subjects under the law;
b) is responsible for ensuring the necessary personal, material and technical conditions for the protection of personal data processed by the University;
c) is responsible for remedying any deficiencies or breaches of law that may be discovered during the control of data processing, and for initiating or conducting any proceedings necessary to establish personal liability;
d) is responsible for complying with the requests of the person concerned;
e) is responsible for the designation and assignment of a data protection officer (DPO) capable of performing data protection tasks, and for notifying the name and contact details of the DPO to the NAIH and informing the DPO thereof;
f) issues a privacy policy;
g) represent the University in relation to requests from external bodies and persons concerning the University's processing of personal data;
h) ensure that the University only uses the services of data processors that process personal data in compliance with the applicable legislation;
i) establishes the responsibilities and powers for data protection and related activities and designates the authorities for the processing of personal data and monitors compliance with these responsibilities and powers;
j) designate the person or persons responsible for supervising the processing;
k) directs and instructs the heads of the University's departments with regard to data management;
l) organise the work of the University's departments in such a way that personal data are processed only by those employees who need to know them in order to perform their duties, and that personal data are not accessible, known, altered or destroyed by unauthorised persons;

m) provide data protection training for employees;
n) is responsible for the compliance with the deadlines set for the deletion of data and for the deletion of data once the deadlines have expired;
o) is responsible for conducting and regularly reviewing data protection impact assessments and for ensuring that the necessary conditions are in place;
p) is responsible for initiating a prior consultation with the necessary impact assessment, depending on the outcome of the data protection impact assessment;
q) is responsible for keeping records of data breaches, notifying the NAIH in a timely manner if the legal conditions are met, and informing the data subjects affected by the data breach.

8.2. **Heads of departments**

8.2.1. The heads of specific departments of the University are responsible for the lawfulness of the processing of data by the departments under their control. The head of a given organizational unit shall determine the organization of data protection in that unit, the tasks and responsibilities for data protection and related activities, taking into account the specific nature of the data management activities, on the basis of the instructions of the Rector.

8.2.2. Heads of department, in relation to the department under their control, in relation to data protection:

a) order a personal data processing investigation;
b) are obliged to forward the requests to the Rector's Office and to cooperate in their execution;
c) forward to the Rector's Office requests from external bodies and persons,
d) are responsible, under the instructions of the Rector, for remedying any deficiencies or unlawful circumstances that may be discovered during the audit of data management, and for initiating or conducting any proceedings necessary to establish personal liability.

8.2.3. The Rector shall assist in the implementation of his/her decision pursuant to Section 8.1.3 (l) and organise the work of the organisational unit under his/her control in such a way that only those employees participate in the processing of personal data who need to do so for the performance of their duties, and that personal data are not accessible, known, altered or destroyed by unauthorised persons.

8.3. **The Data Protection Officer**

8.3.1. The Data Protection Officer may be a person employed by the University or an external service provider who can be designated or trusted to perform the duties of Data Protection Officer. The body or person performing the duties of the DPO shall act under the direct authority of the Rector.

8.3.2. If the DPO is appointed from among the persons employed by the University, the DPO may perform other duties, but the University must ensure that no conflict of interest arises from these other duties and that the performance of other duties does not compromise the DPO's duties.

8.3.3. No person may be appointed as a data protection officer whose relative within the meaning of Act V of 2013 on the Civil Code is a person entitled to take decisions on data processing at the University.

8.3.4. The job description or the contract of engagement of the DPO should include the main tasks to be performed.

8.3.5. The Rector shall ensure that the DPO receives the information necessary to perform his/her duties in a timely manner and that he/she has all the knowledge of the organisation and processes necessary to carry out his/her expert activities. The DPO shall be bound by a duty of confidentiality in the performance of his or her duties.

8.3.6. The DPO shall not be subject to any professional instructions or sanctions in connection with the performance of his or her duties. The DPO shall be responsible to the Rector for the legality of his/her activities and for compliance with professional rules.

8.3.7. The University is obliged to involve the data protection officer in the handling of requests related to data processing and to provide him/her with the necessary information.

8.3.8. Tasks of the Data Protection Officer (DPO)

a) provide information and professional advice to staff carrying out data processing on their obligations under the Regulation and other EU or national data protection provisions;
b) monitor compliance with the Regulation and other data protection provisions and the controller's internal rules on the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in data processing operations, and related audits;
c) investigate the notifications received by the University concerning the data management carried out by the University and, if necessary, make proposals to eliminate the errors and deficiencies identified;
d) cooperate with the supervisory authority;
e) act as a contact point for the supervisory authority on matters relating to data management and consult it on any other matter as appropriate;
f) contributes to the training of persons employed by the University in data protection;
g) carry out the data protection tasks specified by the Rector's Office on a case-by-case basis.

8.3.9. The DPO shall carry out his or her tasks with due regard to the risks associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

8.4. **Persons employed by University involved in the processing**

8.4.1. All persons employed by the University in the performance of their duties shall ensure that no unauthorised person has access to the personal data processed by them in the performance of their duties, and shall ensure that personal data are stored and stored in such a way that they cannot be accessed, accessed, altered or destroyed by unauthorised persons.

8.4.2. A person employed by the University is responsible for the processing, alteration, deletion, transmission and disclosure of data within the scope of his or her duties, and for the accurate and traceable documentation of the data. In the course of his or her duties, he or she shall consult the head of the department prior to the data processing operation, if necessary.

8.4.3. Persons employed by the University shall handle and retain data obtained in the course of their duties or employment, and may only disclose such data if authorised by law or on the instructions of the head of the department, in full compliance with the provisions of the Policy.

8.4.4. Furthermore, a person employed by the University is obliged to keep business secrets disclosed to him/her in the course of his/her work in accordance with Section 8 (4) of Act I of 2012 on the Labour Code. In addition, he/she shall not disclose to any unauthorised person any information which he/she has acquired in the course of his/her employment and the disclosure of which could have a detrimental effect on the University or any other person. Confidentiality shall not extend to the obligation to provide information and to provide information on data of public interest and on data which are in the public interest, as defined by law.

8.4.5. The person employed by the University shall immediately report any irregularity in data management to the head of the department and, if necessary, participate in its rectification.

8.4.6. The person employed by the University shall comply in the course of his or her activities with the legislation on data management and the provisions of this Policy.

8.4.7. A person employed by the University shall process personal data on technical equipment and using software designated by the University. Other hardware and software may be used only with the prior written consent of the Rector.

8.4.8. A person employed by the University is only entitled to transmit personal data files containing personal data through secure channels. If in doubt as to the adequacy of the security of the communication channel to be used, they must seek the instructions of the Head of Department before transmitting the data.

8.4.9. A person employed by the University uses password protection for all devices used to manage personal or business data.

8.4.10. Where possible, data matching should be performed when communicating with the data subject, provided that the communication channel is sufficiently secure.

8.4.11. Persons employed by the University shall participate in data protection training organised by the University.

8.4.12. A person employed by the University shall inform the Head of the department and the DPO of any incident where he or she has been requested or instructed to carry out unlawful processing or has experienced any other unauthorised access or processing of data on his or her own system.

9. Shared data management, data processing, data transfers

9.1.1. Where the University determines the purposes and means of data processing within its scope of responsibility jointly with another University, this shall be considered joint processing. The obligations arising from joint processing are set out in detail in a separate annex under Chapter VIII of the Policy.

9.1.2. 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 Infotv..

A separate Annex under Chapter VIII of the Policy deals with the scope and tasks related to the cases where the University engages a data processor and the cases where the University carries out data processing activities.

9.1.3. 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.

The conditions for both data transfers and transfers to third countries are set out in detail in a separate annex under Chapter VIII of the Policy.

Chapter III

RESPONSIBILITY FOR DATA MANAGEMENT

10. Responsibility of the University

10.1. The University bears the responsibility for the processing of personal data.

10.2. In order to enforce his/her right to judicial remedy, the data subject may bring an action against the University or the processor in relation to processing operations within the scope of the processor's activities before the data protection authority or a court if he/she considers that his/her personal data are processed in breach of the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union.

11. Liability of persons employed by the University

11.1. Persons employed by the University are liable under employment law, civil law and criminal law for the lawfulness of the processing operations carried out in the course of their work and for compliance with the provisions of the Policy.

11.1.1. If a person who has a student relationship with the University processes personal data on behalf of or on behalf of the University or any of its departments, in particular, but not limited to, acting as a member or official of the University Student Government, he/she shall accept the provisions of this Policy as binding on him/her and shall process personal data in accordance with this Policy and the applicable laws. The obligations applicable to employees of the University in such cases shall also apply to persons who are students.

11.2. Failure by an employee to comply with his or her obligations under the Policy and the law on the processing of personal data is considered to be a culpable breach of duty.

Chapter IV

RULES ON RECORD KEEPING

12. Records to be kept

12.1. In accordance with Article 30 of the Regulation, the University shall keep a register of its data processing activities (inventory of data assets), which shall include all data processing purposes and processes of the University and their main characteristics.

12.2. Where the University carries out processing activities, it shall keep records of the processing activities carried out on behalf of its clients in accordance with Article 30 of the Regulation.

12.3. The University also keeps records of the data processors used, the exercise of data subjects' rights and data protection incidents.

12.4. The content of the records to be kept by the University is set out in a separate annex under Chapter VIII of the Policy.

13. Keeping records

13.1. The records in force at the time of entry into force of theis Policy are set out in Chapter VIII of this Policy.

13.2. The Rector is responsible for the accuracy and updating of the records.

13.3. The records shall be kept in paper and/or electronic form, as directed by the Rector, in accordance with the data security rules set out in this Policy.

13.4. The keeping and updating of records is the responsibility of the employee(s) designated by the Rector.

13.5. Employees are obliged to notify the person(s) in charge of keeping the register without delay of any event affecting the content of the register in the course of their work.

Chapter V

THE DATA BREACH

14. Privacy incident occurrence

14.1. In the event of a breach of data security, accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to, or unauthorized disclosure or access of, personal data processed by the University (hereinafter referred to as a "data breach"), the University or any person processing personal data processed by the University under any legal relationship shall follow the relevant internal procedures for the occurrence of a data breach as defined by the University and set out in Chapter VIII of this Policy.

Chapter VI

IMPACT ASSESSMENT

15. Conducting an impact assessment

15.1. If a processing operation envisaged by the University is likely to present a high risk to the rights and freedoms of natural persons, taking into account its nature, scope, context and purposes, the University will carry out an impact assessment prior to the processing.

15.2. The cases in which the University carries out an impact assessment and how the impact assessment is carried out are set out in detail in a separate annex under Chapter VIII of the Policy.

Chapter VII

OTHER RULES RELATING TO THE PROCESSING OF PERSONAL DATA

16. Characteristics of each data management purpose and activity; introduction of new data management purposes or processes

16.1. The detailed rules of the data management processes related to each of the data management purposes at the University are set out in the data management notices published by the University. The University carries out its data processing activities in relation to each of the processing purposes as described in its Data Processing Notices.

16.2. The privacy notices drawn up in relation to each processing operation shall be deemed to be published without any further action or provision, after obtaining the necessary approvals, after signature by the data controller and publication in a manner appropriate to the specific processing operation. The University shall keep a register of the applicable privacy notices as set out in Chapter IV and in a specific annex under Chapter VIII.

16.3. Only the Rector may order the introduction of a new data management process or the modification of an existing data management process.

16.4. An employee who, in the course of performing a task related to his or her job, is required to introduce a new data management process must notify the head of the department.

16.5. An employee who has a need to change the data management process in his or her job must notify the head of the department.

16.6. A new data management process or a change to data management processes will be introduced if it does not conflict with the provisions of the Policy.

16.7. Before introducing a new data management process or changing data management processes, it is necessary to define the main features of data management, in particular:

a) the purpose of the processing;
b) whether that purpose can be achieved by another processing operation;
c) the legal basis for the processing;
d) the range of stakeholders;
e) the scope of data relating to the data subjects;
f) the source of the data;
g) the duration of the processing of the data;
h) the type of data transferred, the recipient and the legal basis for the transfer, including transfers to third countries;
i) the name and address of the controller and the processor, the actual location of the processing and the activities of the processor in relation to the processing;
j) the type of data processing technology used.

16.8. When a new data management process is introduced or an existing data management process is changed, the Rector shall ensure that contracts, records and policies relating to the management of personal data are updated and that the amended and updated data protection documents are made available to the relevant persons. The activities under this point shall be documented in a verifiable manner.

17. Cessation or change of the purpose of the processing

17.1. In order to comply with the principles set out in point 4 of the Policy, the Data Controller will process personal data only for the time necessary to achieve the purpose of the processing. The duration of the processing for each processing operation shall be determined by the Controller before the processing starts, unless the duration of the processing is predetermined by law.

17.2. When the purpose of the processing ceases (i.e. at the end of the processing period), the Controller shall ensure that the personal data processed are erased or transformed in such a way that the data subject can no longer be identified from the data. The latter may mean pseudonymisation or encryption of the processed data. The measure to be taken at the end of the period of processing shall be decided by the Controller on a case-by-case basis, taking into account the specificities of the processing.

17.3. The Controller is entitled to process personal data for purposes other than the original purpose for which they were collected, provided that the processing is compatible with the original purposes for which the personal data were originally collected. Processing for these other purposes constitutes new processing, but does not require a separate legal basis other than the legal basis which originally allowed the collection of the personal data.

In order to determine whether the purpose of the further processing is compatible with the original purpose for which the personal data were collected, the Controller will, after having fulfilled all the requirements relating to the lawfulness of the original processing, take into account, inter alia, any link between those original purposes and the envisaged further processing purposes, the circumstances in which the data were collected, including in particular the reasonable expectations of the data subject based on his or her relationship with the controller with regard to further processing, the nature of the personal data, the consequences of the envisaged further processing for the data subjects and the existence of appropriate safeguards in both the initial and the envisaged further processing operations.

The Controller shall carry out a compatibility analysis of further processing under this point on the basis of Article 6(4) of the Regulation.

17.4. The Controller shall ensure the enforcement of the processing periods in respect of the processing it carries out.

Chapter VIII

PROCEDURING RENDE

1. Internal procedures to follow in the event of a data breach
2. Internal procedures for responding to a request from an interested party

RECORDS

1. Inventory of data assets
2. Register of applications and exercises of rights by interested parties
3. Data protection incident record
4. Register of data processors
5. Article 30 based register kept as a data processor
6. Applicable privacy notices

ADDITIONAL ANNEXES

1. Processing of personal data and special categories of personal data, legal bases for processing
2. Rights of data subjects, their right to a remedy and the exercise of their rights in relation to the processing of personal data after the death of the data subject
3. Joint processing, data processors, data transfers, data transfers to third countries
4. Mandatory content of records, record keeping
5. Conduct an impact assessment

CLOSING:

The creation of the University of Óbuda's Privacy Policy was approved by the Senate at its meeting held on 28 November 2022 with the resolution ..... It enters into force on 1 December 2022.

Budapest, 2022.....

_____

Prof. Dr. Levente Kovács
Rector