Pannon Egyetem
University of Pannonia

Privacy and Data Protection Policy

Adopted by the Senate on: 30th October 2025

Senate Resolution number: 169/2025. (X.30.)

Effective date: 1st December 2025

Person responsible for the maintenance of this Policy: Data Protection Officer of the University of Pannonia

Version: 01

version	date of publication	effective date	date of repeal	Senate resolution number, Board of Trustees resolution number*
00	02.11.2023.	01.11.2023.	01.12.2025	Senate Resolution No. 200/2023. (X.26.)
01	01.12.2025	01.12.2025		Senate Resolution No. 169/2025. (X.30.)

* if the entry into force of the Policy is subject to adoption by the Board of Trustees

Table of Contents

Chapter I 1

GENERAL PROVISIONS 1

1. § 1

Aim of the Policy 1

2. § 1

Scope of the Policy 1

3. § 3

4.§ 3

Purpose of data processing 3

Chapter II 4

THE DATA PROTECTION ORGANISATION OF THE UNIVERSITY 4

5. § 4

Chancellor 4

6. § 5

Data protection officer 5

7. § 7

Manager 7

8. § 10

Person performing data processing operations 10

9. § 10

Data processor 10

10. § 11

Liability 11

Chapter III 12

PROTECTION OF PERSONAL DATA 12

11. § 12

Principles of processing personal data 12

12. § 13

Legal basis and general conditions of processing 13

13. § 15

Purpose limitation 15

14.§ 16
Data protection impact assessment 16
15.§ 17
Prior consultation 17
Chapter IV 18
RULES OF DATA HANDLING, TRANSFER AND PROCESSING 18
16. §..... 18
Joint processing 18
17.§ 18
The University as data controller 18
18. §..... 20
Data disclosure, data transfer 20
General rules 20
Data transfer on the basis of external request 21
Data transfer to the Higher Education Information System 22
International data transfer 22
Data transfer for statistical purposes 23
Processing personal data in the course of scientific research 23
The procedure of data transfer 23
19. § Data processing 24
Chapter V 25
DATA PROTECTION AND DATA SECURITY REQUIREMENTS 25
20. §..... 25
Data security requirements in connection with the protection of personal data 25
21. §..... 27
Security of the data in connection with the operations of the University 27
22. §..... 30
Personal data breach 30
Chapter VI 32
ENSURING RIGHTS FOR DATA SUBJECTS, THE RULES FOR EXERCISING RIGHTS 32
23. §..... 32
Preliminary information 32

24. §.....33
Consent.....33
25. §.....35
Right of access by the data subject.....35
26. §.....36
Right to rectification.....36
27. §.....37
Right to erasure ('right to be forgotten').....37
28. §.....38
Right to restriction of processing.....38
29. §.....40
Right to data portability.....40
30. §.....40
Right to object.....40
31. §.....41
Automated individual decision-making, including profiling.....41
32. §.....41
Lodging complaints directly with the University.....41
33. §.....42
Common rules for exercising the rights of data subjects.....42
34. § Legal remedy.....43
Chapter VII.....44
UNIVERSITY RECORDS AND REGISTERS.....44
35. §.....44
Register of processing activities.....44
36.§.....45
Controller's records.....45
37. §.....46
Processor's records.....46
38. §.....47
Data transfer register.....47
39. §.....48

Internal processing records 48
40. § 49
Employee register 49
41. § 50
Student register 50
42. § 50
Records necessary for the eduID Identity Federation 50
43. § 51
Records kept on the exercise or refusal of the data subjects' rights 51
44. § 52
Register of personal data breaches 52
Chapter VIII 52
PUBLICATION OF DATA OF PUBLIC INTEREST AND THE MANAGEMENT OF REQUESTS TO HAVE ACCESS TO DATA OF PUBLIC INTEREST 52
45. § 52
Publication of data of public interest 52
46. § 52
Rules on access to data of public interest 52
Chapter IX 56
PROVISIONS GIVING EFFECT TO THIS POLICY 56
Chapter X 56
DEFINITIONS 56
Chapter XI 60
TRANSITIONAL AND FINAL PROVISIONS 60

The Privacy and Data Protection Policy (hereinafter referred to as: “Policy”) issued by the University of Pannonia (hereinafter referred to as: ”University”) on the basis of the Organisational and Operational Rules (hereinafter referred to as: “OOR”), Part I Organisational and Operational Rules of Procedure (hereinafter referred to as: “OORP”) approved by the Senate of the University of Pannonia and adopted by the Foundation for the University of Pannonia acting as the operator exercising founders’ and ownership rights (hereinafter referred to as: “Operator”) and on the basis of the resolution by the Board of Trustees on the rules of procedure for adopting the regulations of the University of Pannonia by the Board of Trustees is as follows:

Chapter I

GENERAL PROVISIONS

1. §
Aim of the Policy

(1) The aim of this Policy is to define rules for data processing and thus ensure the informational self-determination and the freedom of information and that the data stored at the University are managed, maintained and forwarded in a legitimate way.

(2) Furthermore, the aim of this Policy is to ensure compliance with the rules on access to data of public interest and data accessible on public interest grounds and with basic provisions on data of public interest to be published mandatorily.

2. §
Scope of the Policy

(1) The scope of this Policy covers all the personal data managed and processed at the University – by any of its faculties, comprehensive organisational units, organisational units and units that do not qualify as organisational units. It also covers the management and processing of all the data generated during the operations of the University and all the data relating to intellectual properties generated during the operations of the University.

(2) Furthermore, the scope of this Policy covers all the data of public interest and data accessible on public interest grounds kept and managed at the University – by any of its faculties, comprehensive organisational units, organisational units and units that do not qualify as organisational units.

(3) The personal scope of this Policy covers any person

a) being in an employment relationship with the University,

b) who has a valid student status with the University (and the relatives of those having a student status with the University), who are doctoral candidates and who take part in adult educational programmes or training programmes organised by the University,

c) who applies for or takes part in a habilitation procedure or a doctoral degree procedure at the University,

d) who uses the library system of the University,

e) who is included in the contracts and agreements concluded by the University,

f) who uses the infrastructure of the University,

g) who participates in the implementation of the projects the University takes part in.

(4) The personal scope of this Policy also covers any person who are not in a legal relationship with the University mentioned in points a) – c) of paragraph (3) above but

a) whose data are processed by the University for the purpose of establishing a legal relationship like this and for career monitoring purposes after the termination of a legal relationship like this,

b) whose data the University is obliged to process after the termination of the legal relationship due to statutory provisions,

c) who files a request with the University for any reason (e.g. requesting data of public interest, requesting general information, etc.).

(5) The material scope of this Policy covers all the data processed by the University, the data considered to be personal information in accordance with the law, data of public interest and data accessible on public interest grounds.

3. §
Legal background

(1) These Rules are governed by the following provisions of law:

a) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as " InfoAct ")

b) 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)

c) Act CCIV of 2011 on National Higher Education (hereinafter referred to as " NHEAct")

d) Act I of 2012 on the Labour Code

e) Act LXVI of 1995 on public records, public archives and the protection of private archival material

f) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

g) Government Decree No 301/2016 (IX. 30.) on the amount of the reimbursement of costs for the fulfilment of a request for data of public interest information

4.§
Purpose of data processing

(1) The University processes personal and special data essential for the normal operations of the institute, in particular for

a) the services provided by the University,

b) applicants and students to exercise their rights and comply with their obligations,

c) carrying out teaching and research activities,

d) scientific activities,

e) funding projects,

f) exercising employer's rights,

g) those employed as teachers or researchers or in other positions to exercise their job-related rights and comply with their obligations,

h) safekeeping the records specified in Chapter VII,

i) establishing, assessing and certifying eligibility to benefits provided by the law or the organisational and operational rules of the University,

j) sending newsletters and career monitoring.

(2) The processed data may be used for statistical purposes and forwarded to the official authority for the management of statistical data.

Chapter II

THE DATA PROTECTION ORGANISATION OF THE UNIVERSITY

5. §
Chancellor

(1) The Chancellor, taking the organisational and operational peculiarities of the University into consideration, defines and manages the University's data protection organisation and directs the fulfilment of the University's privacy and data protection duties, and, as part of this, the Chancellor:

a) may initiate an investigation;

b) assigns and appoints the data protection officer;

c) issues the University's Privacy and Data Protection Policy;

d) takes care of inquiries and recommendations by the supervisory authority;

e) approves data transfer to entities outside the University – except for data provision required by the law or data transfer made possible by the law, where data subjects are not identifiable;

f) ensures that data protection officer will accept no instructions from anybody in connection with his or her activities;

g) ensures the availability of resources that are necessary for the data protection officer to carry out his or her tasks, access personal data and data processing operations and keep up his or her expert knowledge;

h) ensures that the data protection officer gets properly involved in all the matters relating to the protection of personal data in good time.

6. §

Data protection officer

(1) Within his or her functional responsibilities and scope of authority, the data protection officer:

a) cooperates and provides help in making decisions on data processing and ensuring the rights of data subjects;

b) develops and maintains the internal privacy and data protection policy;

c) in cooperation with the Directorate of Legal Affairs and Procurement, provides information to the Chancellor about specific cases, tasks and their execution, and, if required, he or she informs the Rector and the Chancellor on an ad hoc basis;

d) checks compliance with EU and member state laws and regulations as well as the internal regulations on data processing at the University;

e) takes care of inquiries and requests which are received and immediately forwarded by the Directorate of Legal Affairs and Procurement and which are in connection with the processing of the data subjects' personal data by the University and the exercising of their rights;

f) in the event unauthorised data processing is found, requests the manager responsible for data processing and, if necessary, the data processor

to stop such data processing. Furthermore, he or she initiates the steps that need to be taken to remedy possible complaints;

g) provides professional advice when carrying out data protection impact assessment detailed in 14.§;

h) provides professional advice for managing personal data breaches;

i) provides information and advice to managers and those carrying out data processing operations on their obligations specified by the General Data Protection Regulation and other EU or member state data protection regulations and setting up new processes for data processing;

j) keeps in touch with the supervisory authority, performs the University's obligation to report to or notify the supervisory authority in connection with personal data processing in time based on the data received from the various organisational units, participates in the supervisory authority's audits of the University and takes care of any response to the supervisory authority's inquiries. In particular,

ja) if the criteria are met, he or she reports personal data breaches he or she becomes aware of to the supervisory authority;

jb) he or she notifies the supervisory authority of any refused request by data subjects;

jc) contacts the supervisory authority for preliminary consultation if the data protection impact assessment establishes that data processing is likely to result in high risk due to the lack of measures to be taken by the data controller to reduce risks;

k) signs in to the register kept by the supervisory authority.

(2) The data protection officer may have access all the documents that can be related to the data processing activities of the University, request copies of such documents, have an insight into all the data processing activities of the University with respect to personal data, enter the rooms where data processing is carried out and request any employee of the University or those taking part in data processing to provide oral or written information in connection with the data processing activities of the University.

(3) The organisational unit assigned by the Chancellor ensures that the name, postal address and e-mail address of the data protection officer be published on the University's website www.uni-pannon.hu.

(4) During his or her legal relationship with the University and also after the termination thereof, the data protection officer must safekeep all the personal data obtained in connection with his or her activities as well as any and all data, facts, information or circumstance which the data controller or data processor who employs the data protection officer is not obliged to make accessible to the public according to the relevant provisions of the law.

(5) Based on the data sent by the various organisational units, the University employee assigned by the Chancellor for this purpose takes care of the written registers and records specified in Chapter VII in connection with all all the data processing activities of the University (hereinafter referred to as: employee tasked with the maintenance of data processing records).

7. §
Manager

(1) For privacy and data protection purposes, the definition of manager includes:

a) the executives of the University and

b) of the faculties and

c) of the comprehensive organisational units and organisational units,

d) the President of the Students' Union and the President of the Doctoral Students' Union;

e) the Presidents of the Faculty Students' Unions and the Presidents of the faculty representations of the Doctoral Students' Union.

(2) Managers:

a) are responsible for establishing and operating the privacy and data protection system of the organisational unit they manage by implementing standard data protection measures. As part of this, they are responsible for taking measures within their own scope of authority to ensure the personnel, equipment and technical framework necessary for the protection of the

personal data being processed by the organisational unit in connection with their duties and for compliance and ensure compliance with the provisions of this Privacy and Data Protection Policy with respect to the organisational unit they manage;

b) are obliged to perform regular data protection inspections of the activities of the organisational unit they manage and eliminate any possible deficiencies or unlawful circumstances found during such inspections as well as initiate and conduct proceedings necessary to determine personal responsibility in connection with this;

c) in connection with data processing within the functional responsibilities and scope of authority of the organisational unit they manage, they are obliged to

ca) define the purpose and conditions thereof;

cb) make decisions on data processing (including the means to be used);

cc) ensure that their data processing operations are included in the central data processing register, are updated or set aside by issuing a data processing master file as shown in Annex 1 and reporting such operations to the employee tasked with the maintenance of data processing records;

cd) prepare the data processing information sheet as shown in Annex 3 and ensure that it is filed in the central data processing register together with the data processing master file, updated, set aside, published or made known to data subjects.

d) are obliged, before any planned new data processing – especially when new technology is used – to ensure that a data protection impact assessment is completed on the data processing within the functional responsibilities and scope of authority of the organisational unit under their management if the data processing carries a high risk with respect to the rights and freedoms of natural persons. In the course of this, they are obliged to ask the data protection officer for his or her professional advice. Furthermore, before conducting any impact assessment or start any possible related procurement process, they are obliged to check if there is any similar data processing or planned data

processing at the University with a similar high risk, because these data processings can be assessed under one and the same impact assessment;

e) before any planned new data processing, if the data processing is necessary for the purposes of the legitimate interests of the data controller or a third party, they are obliged to ask the data protection officer for his or her advice;

f) are obliged to ensure that the data subjects can exercise their rights with respect to the data processing within the functional responsibilities and scope of authority of the organisational unit under their management;

g) provide data relating to the data processing within the functional responsibilities and scope of authority of the organisational unit under their management to the employee tasked with the maintenance of data processing records for the purpose of managing registers and records specified in Chapter VII;

h) are obliged to carry out the tasks specified in this Privacy and Data Protection Policy and the relevant laws in the case of any possible personal data breach relating to the data processing within the functional responsibilities and scope of authority of the organisational unit under their management;

i) ensure that all the inquiries received from external bodies or persons about the processing of personal data within the functional responsibilities of the given organisational unit are forwarded to the Directorate of Legal Affairs and Procurement and the Chancellor's Office, except for data transfers required by the law or data transfers permitted by the law for statistical purposes;

j) are entitled to ask the data protection officer for his or her cooperation, advice or the cooperation of the Directorate of Legal Affairs and Procurement for making decisions in connection with data processing, for protecting the rights of data subjects and in connection with their obligations in accordance with the instructions on data processing;

k) are obliged to make themselves familiar and fully comply with the privacy and data protection regulations of the relevant laws, this Policy and each and every internal regulatory instrument in the course of processing personal data;

l) ensure that the data protection officer can be involved in all the matters relating to the protection of personal data at the right time and in the right manner.

8. §

Person performing data processing operations

(1) Is obliged to make himself or herself familiar and fully comply with the privacy and data protection regulations of this Data Protection Policy and each and every internal regulatory instrument in the course of processing personal data.

(2) Is responsible for ensuring that personal data are disclosed to those authorised to receive such data within the University.

(3) Is obliged, during his or her legal relationship with the University and also after the termination thereof, to safekeep all personal data obtained in connection with the operations of the University and he or she may not make them public or use them.

(4) Is obliged to inform his or her immediate supervisor without delay of any privacy or data protection problem, deficiency or personal data breach found during the fulfilment of his or her duties.

(5) Cooperates in the execution of or executes data protection measures according to the instructions of his or her supervisor.

(6) Is entitled, through his or her immediate superior, to ask the data protection officer for his or her cooperation or advice for making decisions in connection with data processing, for protecting the rights of data subjects and in connection with their obligations in accordance with the instructions on data processing.

9. §

Data processor

(1) Only data processors who can provide adequate guarantee for taking appropriate technical and organisational measures to ensure data processing complies with the requirements of the General Data Protection Regulation and the

InfoAct and the rights of the data subjects are protected can be used for data processing on behalf of the University.

(2) A written contract must be concluded with the data processors for the performance of this activity. This contract must make provision for what is written in Article 28 of the General Data Protection Regulation and Articles 25/C and 25/D of the InfoAct. This contract must be regulated in accordance with the internal rules for contracting and procurements.

(3) If the data processor, in violation of the contract concluded with him or her, the InfoAct and the General Data Protection Regulation, defines the purposes and means of data processing himself or herself, he or she must be considered as data controller with respect to data processing.

(4) The data processor may use further data processors only if it is not excluded by any law and if the data controller has given a prior ad hoc or universal authorisation in the form of a public instrument or a private document providing full evidence to the use of further data processors.

(5) If the data processor uses further data processors on the basis of the data controller's universal authorisation, the data processor shall, before starting using further data processors, inform the data controller of the fact that further data processors are used and of the tasks planned to be carried out by those data processors. If the data controller, based on this information, raises objection to the use of further data processors, the data processor is entitled to use further data processors only if the criteria specified in the objection are met.

(6) The data controller is responsible for the legitimacy of instructions given to the data processor.

10. §
Liability

(1) The employees of the University or any person in any legal relationship with the University processing personal data as part of their job or while fulfilling their duties have labour-related, civil and criminal liability for the lawfulness of data processing carried out as part of their duties and for non-compliance with the provisions of this Data Protection Policy.

(2) The employee may be held accountable for the following in particular (but not limited to):

a) uses his or her access contrary to the intended purpose (e.g. makes queries out of his or her scope of competence, uses his or her access to let unauthorised people have access, or discloses data to unauthorised people);

b) discloses personal data obtained in a lawful manner in the course of fulfilling his or her duties to unauthorised people or let them have access to such data;

c) violates data protection or privacy provisions (e.g.: lets other people use his or her password; alters or deletes personal data);

d) does not report personal data breaches found at all or reports such breaches but not in time.

Chapter III

PROTECTION OF PERSONAL DATA

11. §
Principles of processing personal data

(1) Personal data at the University:

a) shall be processed lawfully, fairly and in transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (“purpose limitation”);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

e) kept 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ("storage limitation");

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");

(2) The organisational unit responsible for data processing shall ensure that any data processing carried out at the University comply with Section (1) above and be able to demonstrate such compliance ("accountability").

12. §
Legal basis and general conditions of processing

(1) Personal data may be processed if any of the following conditions is met:

a) the data subject has given consent to the processing of his or her personal data for one or more designated purposes,

b) the data processing is necessary for the performance of a contract where the data subject is one of the parties,

c) it is necessary for compliance with statutory obligations of the University,

d) it is necessary for, and proportionate to, the protection of the vital interests of the data subject or of another person, or the elimination or the prevention of a direct threat to the life, physical integrity or property of persons,

e) the data processing is of public interest or is necessary for the performance of duties as part of exercising its powers as a public authority vested on the Universtity,

f) the data processing is necessary for the legitimate interests of the University or a third party, unless the data subject's rights in relation to the personal data in question override such interests.

(2) If the type of data to be processed, the purpose and conditions of processing, the access to such data, the controller and the duration of the processing are determined by Union or Member State law, they must be adhered to in the course of processing by the University.

(3) Sensitive data may be processed if

a) the data subject has given explicit written consent to the processing of the personal data in question for one or more specified purposes, or

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or

c) processing relates to personal data which are manifestly made public by the data subject, or

d) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services,

e) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, on the basis of Union or Member State law which is proportionate to the aim pursued, respects the right to the protection of personal data and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

(4) Prior to the collection of data, the data subject shall be informed, with due regard to the provisions of the General Data Protection Regulation, of the information on the basis of which the data processing is carried out. This shall take the form of the publication of a Privacy Policy.

(5) The data subject shall be informed by the controller by means of a Privacy Notice at the time the personal data are obtained if the controller's organisational unit collects the personal data relating to the data subject directly from the data subject, and within a reasonable period after obtaining the data, but at the latest within one month if the personal data are not obtained from the data subject.

(6) If the processing of sensitive personal data is based on the data subject's consent, the written consent of the data subject must be obtained where the data subject gives his or her consent to the processing of the data specified in the consent for the specified purposes and under the specified conditions, except if the data subject has provided his or her sensitive personal data in his or her written request submitted or submission sent to the University. In such a case, the consent is deemed to be given through the written request or submission for the purposes of the procedure.

(7) Special care must be taken when processing sensitive personal data. Special attention must be paid to ensure that only those can have access to such data for whom it is absolutely necessary to be able to fulfil their duties relating to their data processing operations.

13. §
Purpose limitation

(1) The purpose and conditions of processing are included

a) the Union or Member State law requiring processing or

b) the relevant university privacy notice

the purpose(s) of which must be adhered to in the course of processing.

(2) The data being handled during the various procedures may be processed only with the aim of the arranging the case in question.

(3) The personal data being processed by the University or those made available by other data controllers for the fulfilment of the duties of the University may not be used for private purposes or made accessible to unauthorised people.

14.§

Data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the University shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

(2) The University shall seek the advice of the data protection officer, when carrying out a data protection impact assessment.

(3) A data protection impact assessment referred to in Section (1) shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or

c) a systematic monitoring of a publicly accessible area on a large scale.

(4) The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes of processing;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulation

taking into account the rights and legitimate interests of data subjects and other persons concerned.

(5) Where appropriate, the University may seek the views of data subjects, their representatives or the supervisory authority on the intended processing, without prejudice to the security of processing operations.

(6) Where necessary, the data protection officer shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

15.§
Prior consultation

(1) Before starting the processing of personal data, the data protection officer shall consult the supervisory authority at least 14 weeks prior to the date of the intended processing, if a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(2) When consulting the supervisory authority, the data protection officer shall provide the supervisory authority with the following information:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b) the purposes and means of the intended processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the General Data Protection Regulation;

d) the data protection impact assessment provided; and

e) any other information requested by the supervisory authority.

Chapter IV

RULES OF DATA HANDLING, TRANSFER AND PROCESSING

16. §
Joint processing

(1) Where the University, jointly with one or more other persons or bodies, determines the purposes and means of data processing, the University and these other persons or bodies are considered to be joint controllers.

(2) The head of the organisational unit shall ensure that, in the event of joint processing, the joint controllers conclude a written agreement within the functional responsibilities and scope of authority of the organisational units under his or her management.

(3) Such an agreement shall include their respective responsibilities for compliance with their obligations as data controllers, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information, unless it is determined by Union or Member State law. The controllers shall designate a contact point for data subjects in the agreement.

(4) The essence of the agreement shall be made available to the data subject.

(5) Irrespective of the terms of the agreement, the data subject may exercise his or her rights under the General Data Protection Regulation and the InfoAct in respect of and against each of the controllers.

(6) The head of the organisational unit shall ensure that the Privacy Notice dealing with the processing explicitly names all the controllers and includes their contact information.

17.§
The University as data controller

(1) In accordance with Section (1) of Article 18 of NHEAct, the University may process data for the achievement of the following purposes:

a) the normal operations of the institute,

b) exercising the rights and fulfilling the obligations of students of and applicants to the University,

c) arrangements in connection with training programmes and research projects,

d) exercising employer's rights as well as exercising the rights and fulfilling the obligations of teachers, researchers and employees,

e) keeping records specified by the relevant regulations,

f) assessing, establishing and certifying eligibility for benefits specified in the relevant regulations and the organisational and operational rules of the higher educational institute,

g) processing personal and sensitive data vital for career monitoring in its study management system.

(2) The rules related to data processing are included in the General Data Protection Regulation, the InfoAct, the regulations on data processing and the related internal policies of the University.

(3) Within the organisational system of the University, the controller of data being processed in connection with the operations of the University is always the University.

(4) Personal data may be processed for several purposes within the University's organisational system. The purposes necessary for the processing of personal data may be linked with the tasks of various organisational units of the University.

(5) Within the University's organisational system, the data being handled by the University may be processed only to the extent and for the period of time necessary to achieve all the purposes.

(6) Personal data shall be made available at the University on a hard copy, in a closed envelope, to the hands of the addressee. Data processed in an electronic form may be forwarded as an attachment to an e-mail or on a data storage medium sent to the addressee in a way that the data must be included in a compressed file protected with a password. The password necessary for decompressing must be separated from the compressed file and forwarded as such.

(7) The rules set forth in Section (6) above do not apply to cases when the person authorised to process data forward the data directly to another person authorised to process data on a hard copy.

(8) Employees of the University carrying out data processing activities within the organisational units of the University shall, pursuant to Section (4) of Article 8 of Act I of 2012 on the Labour Code, as well as under any other regulation imposing a duty of confidentiality, keep as confidential – without any time limitation – any personal data that come to their knowledge in the course of their activities. This duty of confidentiality shall not extend to the disclosure of data of public interest or data made public on grounds of public interest, nor to statutory obligations to provide data and information, or to the submission of complaints and public interest disclosures as defined by law.

(9) Upon commencement of employment, new employees of the University shall receive basic data protection information as part of the onboarding package. The induction training and any subsequent training sessions shall be organised by the Directorate of Human Resources Management (hereinafter referred to as "DHRM"). The DHRM shall keep records of employee training, containing the following information:

a) the name of the participant in the training;

b) the date of the training.

18. §
Data disclosure, data transfer

General rules

(1) Personal data may be made accessible to third parties with the aim of transferring or disclosing them.

(2) Personal data may be transferred to a third party only in accordance with the relevant provisions of the law, as part of official proceedings based on statutory requirements or on the basis of the data subject's written consent.

(3) International data transfer is when the data are transferred to a (third) country outside the member states of the European Economic Area (EEA). Data transfer to the EEA member states shall be regarded as transfer within the territory of Hungary.

(4) Disclosure means making the data accessible to anyone.

Data transfer on the basis of external request

(5) Any request for the transfer of personal data being processed by the University can be fulfilled only in accordance with statutory provisions or if the conditions set forth in Section (2) above are met. In any other case, the request for data transfer must be refused.

(6) When the data transfer is based on other than statutory obligations, any request for such transfer may be fulfilled only if the data subject gives his or her unambiguous consent in an express written declaration of consent, authorising the University to transfer the data. The data subject can also give a preliminary authorisation which can be for a specific period of time or a group of bodies that may send such requests. If a student makes a proper declaration in his or her personal, password-protected account in the Electronic Academic Administration System, it shall be considered as an unambiguous consent by the student. Anybody who is in an employment relationship or has a student status with the University and submits an application to an external competition through the University must submit an express declaration of consent with their application, so that the University can forward the personal data related to competition to the announcer of the competition or the organisation authorised to supervise the application, implementation and settlement of the competition.

(7) Any facts or circumstances relating to the data provided in response to a request shall be documented in a record prepared by the organisational unit performing the data transfer.

(8) No records have to be prepared for data transfers where the transfer of data is genuinely verifiable in any other way. For example, no records have to be prepared where the request is sent in a written form and filed by the competent organisational unit and the data transfer is implemented through a registered written document.

(9) External requests may only be completed by the organisational unit authorised to transfer data. With respect to the data of persons specified in Points b)-c) of Section

(3) of Article 2, the competent organisational unit is the one performing tasks in connection with the organisation of education, while in the case of the personal data of persons specified in Point a) of Section (3) of Article 2, it is the organisational unit managing employment affairs and, regarding the personal data of persons specified in Points a)-b) of Section (4) of Article 2, it is the organisational unit performing tasks in connection with the organisation of education or the organisational unit managing employment affairs. In the case of any other requests for data, the Chancellor's Office shall have competence. If an external body or private person sends a request for data transfer to an unauthorised organisational unit or employee, the organisational unit or employee in question shall forward the request to the Chancellor's Office.

(10) Before any data transfer, the controller or the processor acting on behalf of or instructed by the controller inspects the accuracy, completeness and up-to-dateness of the personal data to be transferred.

Data transfer to the Higher Education Information System

(11) Taking the provisions of Section (1) of Article 19 of the NHEAct, the University shall transfer data to the Higher Education Information System.

(12) The Rector assigns designated person(s) at his or her own discretion to certify electronic data transfer to the Higher Education Information System.

International data transfer

(13) In the event of international data transfer, the person transferring data shall ensure that the conditions of international data transfer as specified in the InfoAct are fulfilled. As part of this, it shall be checked if the data are transferred in accordance with any of the legal bases set forth in the InfoAct and the adequate level of protection of the data is provided by the controller receiving the data. If the data are transferred to any member state of the European Economic Area, the adequacy of the level of protection of the personal data does not have to be verified.

Data transfer for statistical purposes

(14) The University undertakes to hand personal data over for statistical purposes only if it is ensured that they cannot be linked with the data subject.

Processing personal data in the course of scientific research

(15) Personal data being managed for scientific research purposes may be used only for scientific research.

(16) Any connection between the personal data and the data subject, as soon as the research purpose allows it, must be made permanently unidentifiable. Until this happens, the data that are suitable for the identification of a designated or identifiable natural person. Such data may be linked with other data only if it is necessary for research purposes.

The procedure of data transfer

(17) At the University, personal data may be disclosed to the extent necessary for performing the task and only to an organisation unit or person taking part in data processing that needs to know and handle the personal data for performing their tasks specified in the internal control system of the University.

(18) Data may be transferred to a designated third party outside the University if

a) the University is the controller of the personal data or has received it from another controller and it is not under any restrictions; and

b) the data subject has agreed to the data transfer or the data must be transferred to a body or person specified in Union or Member State law in the data category set forth therein; and

c) when the data are transferred to a third country or an international organisation, the European Commission has issued a Declaration of Conformity in connection with the third country or international organisation or, for lack of such a declaration, the supervisory authority has approved the data transfer; and

d) the Chancellor has approved the transfer of data to outside the University – except for data transfers required by the law or when the data are allowed by the law to be transferred for statistical purposes.

(19) The fulfilment of conditions set forth in Section (2) above must always be checked by the person carrying out the data transfer on behalf of the University before the data are transferred.

(20) The information necessary for the approval of data transfer, including the addressees, the purpose and legal basis of data transfer, a precise description of the data requested, the data subjects and, in the case of international data transfer, the country where the data are transferred to, as well as the proposal for decision are provided by the manager submitting the requests.

(21) The head of the organisational unit responsible for data processing shall inform the employee tasked with managing the data processing register of any data transfer completed to a third party on the basis of a request by filling in the Data Processing Registry Sheet enclosed as Annex 1 herewith (completing field I. (Data Controller), field II (Internal identification number necessary for identifying data handling and description of data handling) as well as field VI. (Data Transfer)). This employee then posts the data transfer in the University data transfer register.

(22) Personal data my only be disclosed with the prior consent of the data subject or if it is mandatory by virtue of Union or Member State law.

(23) Data may be provided for statistical purposes only in a way that ensures that no link can be restored between the data subject and his or her data.

19. § Data processing

(1) Only persons or organisations that provide sufficient guarantees to implement appropriate technical and organisational measures suitable for ensuring the protection of the rights of the data subjects may act as data processors.

The processor shall verify these guarantees to the controller prior to the start of processing.

Chapter V

DATA PROTECTION AND DATA SECURITY REQUIREMENTS

20. §

Data security requirements in connection with the protection of personal data

(1) The data processing activities of the University involve everybody who, in any legal relationship with the University, has access to and use the data processed by the University when performing their tasks and manage the registers that include such data. The persons taking part in the University's data processing activities shall treat the personal data they become aware of as secrets. Only those persons may participate in the University's data processing activities who have made a confidentiality declaration as stipulated in their employment contract and in accordance with the provisions set out in the relevant Joint Directive of the Rector and the Chancellor.

(2) The processor entitled to take part in the University's processing activities shall ensure the security of the data within their own sphere of activities and plan and implement the data processing operations in a way that the protection of the privacy of the data subjects be ensured during such operations.

(3) Appropriate measures must be taken to protect the data, in particular, against unauthorised:

a) access,

b) alteration,

c) transfer,

d) disclosure,

e) erasure or destruction,

f) accidental destruction or damage,

g) becoming inaccessible due to the change of the technical means used.

(4) An employee of the University, or a person engaged in an employment-related legal relationship with the University, shall be obliged, on the basis of the provisions of the InfoAct, the General Data Protection Regulation and this Policy, to store

documents containing data classified as personal data outside working hours, and where possible during working hours as well, in a locked cabinet. Official documents may be kept on desks or elsewhere in the office solely for the purpose of performing work and only for the duration thereof. Responsibility for securing the documents lies with the administrator in whose possession the documents are at the end of working hours.

(5) In addition to other considerations, premises in which a shared printer or photocopier is operated shall be used with due regard to data protection considerations and data security requirements.

(6) Premises in which a computer or workstation is operated shall be used in a manner that complies with data protection, fire safety and IT security requirements. The administrator shall be obliged to handle and store the computer and any data carriers used in such a way that data requiring protection cannot be accessed by unauthorised persons. Furthermore, upon completion of working hours, the administrator shall switch off the workstation – except for workstations that must remain continuously powered on and online – and shall lock the door.

(7) Documents containing personal data may be taken out of the University's premises – except for the performance of job-related duties – only with the permission of the immediate supervisor. In such cases, the administrator shall also be obliged to ensure that the documents are not lost, damaged or destroyed, and that their contents do not become known to unauthorised persons.

(8) Access to documents containing personal data that are held by the administrator or in the archives shall be permitted, in addition to the administrator and the administrator's manager, to other persons only if permitted by law, or if the administrator certifies in response to a request addressed to them that the performance of tasks related to their activities necessitates such access.

(9) In the absence of statutory authorisation, data may be transferred to a third party only with the consent of the data subject. If the data subject does not consent to the transfer of their data to another body, they shall be informed that their request cannot be fulfilled or cannot be fulfilled in full. In the case of data transfers within the University, the requesting party shall in all cases be obliged to justify the purpose and legal basis of the data request.

(10) For the protection of data sets managed in various registers and records in an electronic way, appropriate technical means must be provided to ensure that no

direct connection between the data stored in such registers or records and the data subject can be established, unless it is permitted by law.

(11) Personal data must be immediately be deleted after the purpose of processing has been achieved. The heads of the various organizational units are responsible for the security of the data stored at their organizational units. Any hard-copy or electronic document containing personal data may be stored in a way – in particular through the permanent surveillance of the rooms, offices and IT equipment used for storing documents – that no unauthorized people can have access to the data.

(12) During data collection and further data processing, due care shall be taken to ensure the accuracy, completeness and timeliness of personal data, so that the rights of the data subjects are not infringed as a result.

(13) When exercising the right of access by the data subject or their representative, procedures shall be carried out in such a way that the rights of others are not infringed (personal or protected data relating to other persons shall be redacted or otherwise rendered unrecognisable). The same procedure shall be followed when making copies or extracts.

(14) Data that are no longer necessary for achieving the purpose of data processing, as well as data for which the purpose of data processing has ceased or changed, shall – in accordance with the provisions of the Document Management Regulation – be destroyed without delay or upon expiry of the prescribed retention period. The destruction of other document materials containing personal data shall likewise be carried out with the necessary security measures in place.

(15) Personal and special category data recorded in paper-based notes that do not form part of an official case file shall be rendered unidentifiable in order to prevent their further use. Working copies generated during IT processes, as well as spoiled or otherwise unnecessary copies, shall be destroyed.

21. §

Security of the data in connection with the operations of the University

(1) Any person being in an employment relationship with the University shall treat in a purpose-limited and confidential manner every and all data, information, documents or any conclusions drawn therefrom – regardless of the way and form

they were obtained in – that became known to him or her in the course of performing their tasks relating to or in connection with his or her legal relationship or the disclosure of which to a third party could harm any of the University's interests. Such persons shall be liable for any loss or damage arising from the breach of their obligations.

(2) The organisational unit responsible for processing, together with the head of the organizational unit responsible for operating the IT system in the case of electronically-managed data, shall take all the technical and organizational measures as well as have rules of procedure in place which can ensure the security of the personal data managed manually or stored and processed in the computer system.

(3) Personal data must be protected, in particular, against accidental or unlawful destruction, alteration, unauthorised disclosure, unauthorised access or becoming inaccessible. The University applies appropriate procedures to prevent, detect, report and investigate data breaches.

(4) For ensuring protection for personal data,

a) all the documents and data storage media must be stored in a lockable place; offices and cabinets must be locked;

b) the IT systems and work stations where personal data are stored in must be protected with a firewall and regularly updated antivirus software;

c) any access to the personal data stored in servers must be logged, so that at any time it can be clearly seen who had access to what personal data and when;

d) the passwords used for accessing university systems must be especially protected; they must not be disclosed to anyone and must be changed at regular intervals;

e) when leaving workstations, the user must log out;

f) documents containing personal data must be destroyed in a document shredder; they must not be disposed of in waste collectors;

g) documents containing personal data may leave the territory of the University only if duly justified. The employee taking the document away or the person responsible for the processing operations shall be responsible for safekeeping the document and ensuring that it will be kept in good condition;

h) IT equipment or data storage media containing personal data may leave the territory of the University only if they are protected with a password and appropriate encryption methods. The employee taking the equipment or medium away or the person responsible for the processing operations shall be responsible for safekeeping them and ensuring that they will be kept in good condition.

i) Prior to the reuse (in particular sale or leasing) of IT equipment and data carriers containing personal data, and upon their disposal, the personal data stored on them must be irreversibly and permanently deleted.

(5) The scope of data to be stored in the IT systems are determined by the head of the organisational unit responsible for operating the given IT system, taking the relevant statutory requirements and the organisational, financial and IT peculiarities into account. It is the head of the organisational unit responsible for operating the IT system that determines what access right and to what extent access authorisation is given and ensures that access rights be provided. When developing the system of access control, the principle of purpose limitation must be taken into account, with special focus on ensuring that only those persons can have access to the data for whom it is absolutely necessary to be able to fulfil their duties relating to their data processing operations.

(6) To provide access to the data of the IT system, the head of the organisational unit responsible for operating the given IT system may use a form where he or she may require the person for whom access is to be provided (or modified) to provide personal data necessary for identification and the data relating to his or her functional responsibilities necessary for the assessment of eligibility for access, together with proof for such data.

(7) Access to IT systems can be requested by the head of the organisational unit where the person needing access rights belongs to with the head of the organisational unit responsible for operating the given IT system and it is the head of the organisational unit requesting access that must immediately request the withdrawal of access rights when the criteria for having access are no longer met.

(8) Access to the IT systems may be granted to persons who are not in an employment or work-related contractual relationship only if they are involved under a contract in the system development and operation of the IT systems, or if they are authorised under internal regulations with regard to student benefits. The University may, in accordance with a separate directive or regulation, provide e-mail access to

users who are not in an employment relationship, work-related contractual relationship or any other legal relationship with the University, but who, through their activities, contribute to the work of the University community.

(9) The right of access may be used only for performing tasks within one's job description (or as specified by their contract).

(10) In any other matter, data processing is subject to the Information Technology Regulation, the Disposal Policy of the University of Pannonia and the Document Management Policy.

22. §
Personal data breach

(1) Anyone who notices that data processed at the University are lost, probably destroyed, altered, compromised by unauthorised disclosure or unauthorised access shall immediately, at the time when the breach is detected, inform the head of the organisational unit responsible for processing.

(2) The head of the organisational unit

a) shall, at the time when the breach is detected, inform the data protection officer;

b) shall, without delay after the breach was detected, initiate an internal investigation into all the circumstances of the case, involving the data protection officer and, if needed, the Directorate of Information Technology and the Directorate of Legal Affairs and Procurement;

c) shall, without delay after the breach was detected, take the necessary steps to remedy the personal data breach, including the mitigation any adverse legal consequences;

d) based on the findings of the internal investigation, shall, after the personal data breach was detected, make a written report in accordance with Annex 2 to the data protection officer within a time limit that makes it possible for the data protection officer to makes his or her report to the supervisory authority or, if the University acts as data processor, the data controller within 72 hours of taking notice of the breach or as set forth in the Data Processing Agreement but, in any case, during normal working hours;

e) depending on the findings of the internal investigation, after having consulted the data protection officer, if the circumstances of the personal data breach creates a statutory obligation

ea) shall inform the data subjects of the nature of the personal data breach in a clear and easily understandable way, without undue delay,

eb) shall, at the same time, inform the data subjects of the name and contact information of the data protection officer or other contact persons who can give further information,

ec) of the probable consequences of the personal data breach, and

ed) of the measures taken or planned to be taken to remedy the personal data breach, including those steps that are aimed at mitigating the possible negative consequences of the personal data breach.

(3) In the event of failure to meet the deadline specified in Section (2), the head of the organisational unit concerned shall prepare a memorandum for the Chancellor detailing the circumstances of the missed deadline. The Chancellor shall determine the further measures to be taken after obtaining the opinion of the Data Protection Officer.

(4) Based on the report received, the data protection officer

a) registers the breach reported to him or her;

b) shall make a decision within 48 hours of the notification as to whether the University is subject to a reporting obligation in relation to the incident.

ba) If the University is subject to a reporting obligation towards the data protection authority, the report shall be prepared for decision-making by the Chancellor in such a way that, where possible, the report is submitted within 72 hours of becoming aware of the incident, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

bb) Sends a report to the supervisory authority or the data controller, if possible, within 72 hours of taking notice of the breach, except if the personal data breach will in all likelihood not result in risks with respect to the rights and freedoms of natural persons.

(5) If no report is made to the supervisory authority within 72 hours, the reasons for the delay must also be enclosed. The head of the organisational unit responsible

for data processing shall provide all the reasons for delay within his or her scope of activities to the data protection officer.

(6) In the course of the risk assessment of the data breach, the Data Protection Officer shall examine:

a) the nature of the personal data breach,

b) the categories and approximate number of data subjects concerned,

c) the categories and approximate number of personal data affected by the breach,

d) the likely consequences resulting from the breach,

e) the measures taken or planned to address the breach, including, where applicable, measures intended to mitigate any possible adverse effects resulting from the breach.

Chapter VI

ENSURING RIGHTS FOR DATA SUBJECTS, THE RULES FOR EXERCISING RIGHTS

23. §
Preliminary information

(1) Before data processing is started, the data subject shall be given clear and detailed information in connection with all the facts relating to the processing of his or her data. The provision of such data must be documented and, if necessary, the head of the organisational unit responsible for processing shall present proof of this.

(2) Preliminary information must be provided with special respect to the criteria defined in Annex 3, if necessary, supplemented with the special requirements set forth in the various sectoral policies and in line with the information included in the data processing information sheet.

As part of this, a simple and clear choice of words is to be followed for easily understandable texts and the processing, before any change to processing, must be sent to the data protection officer in an editable Word format, together with the data processing master file.

(3) To provide direct information to the data subjects, the manager in charge shall ensure that the privacy and data processing manuals included in the internal data processing register are directly made known to the data subjects in a documented way or, if informing the data subjects directly is impossible or requires disproportionate costs, the manager shall publish such manuals on specific privacy and data processing communication interfaces available to the data subjects.

(4) Where the University or any of its organisational units collects personal data relating to the data subject directly from the data subject, the data controller shall inform the data subject by means of a privacy notice at the time the personal data are obtained; and where the data are not obtained from the data subject, such information shall be done within a reasonable period after obtaining the data, but no later than one month thereafter.

(5) The University may provide information to data subjects in two ways:
a) by means of a general privacy notice, which serves as a summary of the University's data processing activities (including data processing related to employees, students, research activities, and data processing involving personality rights protected by specific legislation);
b) by means of a specific privacy notice, which describes individual data processing activities separated by purpose (e.g. questionnaires, events).

(6) The University shall make information about its data processing activities available to data subjects by publishing the privacy notices on its website. The organisational unit carrying out the data processing is responsible for ensuring such publication.

24. §
Consent

(1) Consent means and is acceptable in the form of any freely given, explicit, specific, informed and unambiguous affirmative statement by the data subject, by which he or she unambiguously signifies agreement to the processing of personal

data relating to him or her, such as by a written statement, including by electronic means. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

(2) Consent may be used as a legal basis only for data processing where compliance with the requirements of prior information and the voluntary nature of the consent can be demonstrated. Voluntariness cannot be demonstrated if consent to data processing serving exclusively the interests of the University is obtained in a relationship of subordination, on a mass basis, within a defined group of persons and without exception from the data subjects.

(3) Consent may be given in any form that allows the data subject to be identified and ensures that the fact of consent is recorded. Consent may not be given orally or by telephone.

Documented forms of accepting consent include, in particular:

a) in writing (with the data subject’s signature);
b) electronically, following individual identification of the data subject (e.g. identification via the student administration system), provided that the fact of consent is recorded (logged);
c) by electronic means, in a message sent from the data subject’s electronic mail address registered with the University, provided that the unchanged recording and retention of the message are ensured.

(4) Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them one by one.

(5) Consent by the data subject in connection with personal data provided by the data subject is presumed to be given for proceedings to be conducted at the request or initiative of the data subject. If possible, the data subject’s attention should be called to this fact.

(6) When processing is based on the data subject’s consent, the processing of the personal data of a child below the age of 16 shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Therefore, in the case of a child below the age of 16, the affirmative consent must in each case include the written declaration of consent given by the parent

having parental responsibility over the child. This means that it is not enough if the parent simply signs the statement for the child.

(7) The data-controlling organisational unit shall ensure that, with regard to data processed on the basis of consent, the duly documented declarations of consent are obtained, properly recorded and stored, and that the data processed on the basis thereof are identified and, in the event of withdrawal of consent, erased in accordance with the provisions set out in Section 27.

25. §
Right of access by the data subject

(1) It is the University's duty to consider the data subject's request for information without undue delay but in no case later than twenty-five days and give confirmation whether or not personal data concerning him or her are being processed, and, where that is the case, it is the University's duty to provide access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria use to determine that period;

e) the existence of the right of the data subject to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

i) appropriate safeguards when data are transferred to a third country or international organisations.

(2) The Directorate of Legal Affairs and Procurement is obliged to provide information at the request of the data subject, after the Chancellor's Office has been informed, on the basis of the information provided by the University's organisational unit responsible for data processing.

(3) If the University processes a large amount of information relating to a data subject, it may ask the data subject, before providing information to the data subject, to clarify which information or processing activities his or her request is for.

(4) If the data request has submitted his or request in an electronic form, the information must be provided in a widely-used electronic format, unless otherwise requested by the data subject.

(5) The requested information must be provided free of charge if the person requesting information has not submitted any request for information to the University in the same category of data in the current year. The University may charge a reasonable fee for any further copies requested by the data subject, which fee is to be based on the actual administrative costs and determined in accordance with the provisions of Secdtion (15) of Article 46 of this Policy. Any information must be provided without prejudice to the rights of other data subjects relating to the protection of their personal data.

26. §
Right to rectification

(1) It is the University's duty to consider the data subject's request for rectification without undue delay but in no case later than twenty-five days and, if the request is justified, rectify or supplement the inaccurate or incomplete data relating to the data subject. The measures for rectification must be taken by the organisational unit responsible for processing.

(2) The University's organisational unit responsible for processing shall inform

a) the data subject submitting a request, and

b) all other recipients who have been provided with the data to be rectified or supplemented of the rectification or supplementation of the data, unless this proves to be impossible or involves disproportionate efforts. At the data subject's request, the University's organisational unit responsible for processing shall inform the data subject of other recipients mentioned in point b) of paragraph (2) herein.

27. §

Right to erasure ('right to be forgotten')

(1) It is the University's duty to consider the data subject's request for erasure without undue delay but in no case later than twenty-five days and, if the request is justified, erase the personal data relating to the data subject.

(2) The University's organisational unit responsible for processing shall erase personal data relating to the data subject without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the period of processing specified by the law has expired;

c) the data subject withdraws consent or there is no other legal ground for the processing;

d) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing aimed at direct marketing activities;

e) the personal data have been unlawfully processed;

f) the personal data have to be erased for compliance with a legal obligation in Union or Member State law;

g) the erasure has been ordered by a court or supervisory authority.

(3) The data may not be erased even at the request of the data subject or if any of the grounds listed in Section (2) above is met where the processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for the establishment, exercise or defence of legal claims;

d) certain special personal data must be processed for reasons of public interest in the area of public health in accordance with the General Data Protection Regulation;

e) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.

(4) Pursuant to the relevant provisions of Act LXVI of 1995 on public records, public archives and the protection of private archives, personal data stored on storage media to be placed in the safe custody of archives may be erased at the request of the data subject only if the data are unlawfully processed. In such a case, the data must be erased irrespective of any other circumstances.

(5) The organisational unit responsible for processing shall take the necessary measures to document all the decisions and facts in connection with the erasure of data and the discontinuation of processing.

(6) The University's organisational unit responsible for processing shall inform

a) the data subject submitting a request, and

b) all other recipients who have been provided with the data to be erased of the erasure of the data, unless this proves to be impossible or involves disproportionate efforts.

(7) At the data subject's request, the University's organisational unit responsible for processing shall inform the data subject of such recipients.

28. §
Right to restriction of processing

(1) It is the University's duty to consider the data subject's request for restriction of processing without undue delay but in no case later than twenty-five days and, if

the request is justified, restrict the processing of personal data relating to the data subject, if

a) the accuracy of the personal data is contested by the data subject, for a period necessary for verification;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, however they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pursuant to Article 21 (1) of the General Data Protection Regulation; in such a case, the restriction of processing is limited to the period that is necessary to verify whether the legitimate grounds of the controller override those of the data subject.

(2) The methods used to restrict the processing of personal data include, in particular, the temporary relocation of personal data into another data processing system or the discontinuation of access to such personal data by the persons carrying out processing operations or the temporary removal of data made available on a website. The processing must be basically restricted by technical means in a way that no further processing operations can be performed on the personal data and they cannot be altered. The fact that the processing of personal data is restricted must be clearly indicated in the system.

(3) The University's organisational unit responsible for processing shall ensure the restriction of processing.

(4) Where processing has been restricted, such personal data shall only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(5) The University's organisational unit responsible for processing shall inform

a) the data subject submitting a request, and

b) all other recipients who have been provided with the data to be restricted of the restriction of processing and of lifting such restriction, unless this proves to be impossible or involves disproportionate efforts.

(6) At the data subject's request, the University's organisational unit responsible for processing shall inform the data subject of such recipients.

29. §

Right to data portability

(1) Where the processing of personal data is carried out by automated means or is based on the data subject's consent or is necessary for the performance of a contract concluded by the data subject or the implementation of pre-contractual measures, it is the University's duty to provide the data subject, at the data subject's request, with the personal data made available to the University by the data subject in a structured, commonly used, machine-readable and interoperable format without undue delay but in no case later than twenty-five days. The data subject has right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

(2) The data subject shall have the right to request his or her personal data being transmitted directly from one controller to another.

(3) The right to data portability shall not apply when the 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 University.

30. §

Right to object

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on the performance of a task carried out in the public interest or in the exercise of official authority or to processing aimed at enforcing legitimate interests, including profiling.

(2) The processing of personal data in cases specified in Section (1) above may be continued against the data subject's objection only if the University's organisational unit responsible for processing demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(3) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. In such a case, the personal data shall no longer be processed.

(4) Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

31. §
Automated individual decision-making, including profiling

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except if the decision

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;

c) is based on the data subject's explicit consent.

(2) In the cases referred to in points (a) and (c) of paragraph 1 above, the data subject shall have the right to obtain human intervention on the part of the University, to express his or her point of view and to contest the decision. The University's organisational unit responsible for processing shall ensure that the data subject can exercise such rights of his or hers.

32. §
Lodging complaints directly with the University

(1) The organisational units responsible for processing shall, by publishing their contact information, ensure the data subject can lodge his or her complaints directly with the University's organisational unit responsible for processing in connection with any processing activity of the University, if the data subject believes that his or her rights have been infringed as a result of the processing of his or her personal data or such infringement is imminent.

33. §

Common rules for exercising the rights of data subjects

(1) Any and all persons carrying out data processing operations at the University shall facilitate the exercise the rights of data subjects.

(2) Data subjects may directly contact the University's organisational unit responsible for processing regarding the exercise of their rights. In this case, the organisational unit responsible for data processing shall forward the data subject's request or inquiry to the Data Protection Officer. If the data subject does not know which organisational unit of the University is responsible for processing, then he or she can also contact the data protection officer of the University via the contact information published on the website of the University.

(3) As a rule of thumb, only general information may be provided to data subjects over the phone in connection with their rights and the exercise of their rights. The University accepts statements or requests in connection with exercising the rights of data subjects, including requests for information on their personal data, basically in writing, in an electronic form or by post. If there is doubt whether a specific request is from the data subject concerned, the requestor's eligibility must be verified.

(4) The University may request the data subject, before providing information to the data subject, to clarify which information or processing activities his or her request is for.

(5) Where the University has reasonable doubts concerning the identity of the natural person making the request, the University may request the provision of additional information necessary to confirm the identity of the data subject.

(6) The University's organisational unit responsible for processing shall provide information on action taken on a request to the data subject without undue delay and in any event within 25 days of receipt of the request. That period may be extended by

further 60 days where necessary, taking into account the complexity and number of the requests. The University's organisational unit responsible for processing shall inform the data subject of any such extension within 25 days of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(7) If the University's organisational unit responsible for processing fails to take action on the request of the data subject, the unit shall inform the data subject without delay and at the latest within 25 days of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

(8) The data subject and those to whom the data have earlier been forwarded to for processing shall be informed of any rectification, supplementation, restriction or erasure. Such informing can be omitted if such omission does not violate the legitimate interests of the data subject with respect to the purpose of processing.

(9) Union or Member States law may restrict the scope of the data subject's rights and the scope of the rights and obligations provided for in the principles of data processing in so far as its provisions correspond to the exercise of rights by the data subject.

(10) Information on and measures in connection with the circumstances of processing, exercising the rights of data subjects and personal data breaches shall be provided to the data subjects by the University free of charge. If the data subject's request is undoubtedly ungrounded or, due to its repeated nature, exaggerated, the University may refuse to take action on the request in consideration of the administrative costs of providing the information or taking the action requested.

(11) The University and the organisational unit in charge shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(12) Where the data subject's request is for the provision of further copies, the University may charge a reasonable fee based on administrative costs.

34. § Legal remedy

(1) The data subject may lodge a complaint in connection with any processing by the University directly with a supervisory authority if the data subject believes that the University violates the General Data Protection Regulation in the course of processing the personal data relating to the data subject. For any entity subject to the laws of Hungary, the scope of responsibilities and competence specified for the supervisory authority in the General Data Protection Regulation is exercised by the National Authority for Data Protection and Freedom of Information (postal address: 1055 Budapest, Falk Miksa street 9-11, phone number: +36-1-394-1400; website: www.naih.hu; email: ugyfelszolgalat@naih.hu).

(2) The data subject may directly address the court in connection with any processing by the University if the data subject believes that the University violates the General Data Protection Regulation in the course of processing the personal data relating to the data subject. The case shall be judged by a regional court. The data subject may bring the action, at his or her discretion, before the regional court that has jurisdiction in the region where he or she resides in (the list and contact information of the regional courts can be found via the following link: http://birosag.hu/torvenyszekek).

Chapter VII

UNIVERSITY RECORDS AND REGISTERS

35. §
Register of processing activities

(1) The University of Pannonia shall keep records of the data managed by it as data controller or data processor to demonstrate compliance with the General Data Protection Regulation and the InfoAct with respect to the data handling and processing activities within its scope of competence. The University shall cooperate with the supervisory authority and make such records available upon request, so that the data processing operations in question can be supervised.

(2) The records and documents required by this Policy shall be maintained and prepared by the Data Protection Officer. The head of the organisational unit handling

the data is responsible for the completeness of the records, the accuracy and up-to-dateness of the data contained therein and for providing the records to the Data Protection Officer. The data processing records are maintained and stored centrally by the University, acting as data controller, through the Data Protection Officer, based on the data provided by the heads of the organisational units responsible for processing.

(3) The head of the organisational unit managing data sets for registry purposes shall notify the Data Protection Officer of establishing a new data set before commencing the activity. If the Data Protection Officer determines during their activities that the processing of personal data requires maintaining a registry, he or she shall inform the head of the organisational unit and provide methodological support to carry out tasks related to the registry.

(4) The data processing registry shall include records of data processing for all organisational subunits according to the internal structure of the organisational unit. The organisational unit shall examine the content compliance and up-to-dateness of the published records through built-in process controls, and the Data Protection Officer shall verify them through inspections. If necessary, the organisational unit shall supplement or modify the data processing registry. In the event of terminated data processing, the organisational unit shall archive the data processing registry, and, in the case of new data processing, a new data processing registry shall be established.

36.§
Controller's records

(1) The University's records kept as controller includes the following information:

a) the name and the contact details of the controller, including each joint controller, as well as of the data protection officer,

b) the purpose or purposes of processing,

c) in the event of the transfer or planned transfer of personal data, the scope of the recipients of the data transfer, including recipients in third countries and international organisations,

d) the scope of data subjects and of the data processed,

e) in the event of profiling, the existence of it,

f) in the event of international data transfer, the scope of the data transferred,

g) the legal bases of the processing operations, including data transfer,

h) where known, the time for the erasure of the personal data processed,

i) the general description of the technical and organisational security measures implemented,

j) the circumstances of personal data breaches that occurred in the context of the data that it processes, as well as their effects and the measures taken to address them,

k) the legal and factual reasons for its measures restricting or rejecting, according to this Act, the enforcement of the data subject's right of access.

37. §

Processor's records

(1) The University's records kept as processor includes the following information:

a) the name and the contact details of the controller, the processor and of other processors, as well as of the processor's data protection officer;

b) the types of processing operations carried out on behalf of, or according to the instruction given by, the controller;

c) in the event of international data transfer implemented according to the controller's explicit instruction, the existence of international data transfer, as well as the indication of the recipient third country or international organisation;

d) the general description of the technical and organisational security measures implemented.

(2) For the purpose of ensuring the verifiability of the lawfulness of processing operations carried out with personal data by electronic means, the employee tasked with keeping processing records shall record the data processed as controller and

processor in an automated processing system (hereinafter referred to as: “electronic logbook”), including

a) the scope of the personal data affected by the processing operation,

b) the purpose of and the reason for the processing operation,

c) the exact time of carrying out the processing operation,

d) the person carrying out the processing operation,

e) the recipient of the data transfer if data transfer is implemented.

(3) The data recorded in the electronic logbook may only be accessed and used for the purpose of verifying the lawfulness of processing and enforcing data security requirements, as well as conducting criminal proceedings.

(4) At the request of the Authority or a person or organisation engaged in an activity specified by the law for a purpose described in paragraph (3), the controller and the processor shall provide access to the electronic logbook and shall transfer data from the logbook to the requesting party.

(5) The data recorded in the controller’s and the processor’s records, as well as the electronic logbook, shall be retained for ten years after the erasure of the processed data.

38. §
Data transfer register

(1) The organisational unit performing processing activities maintains a register of the transfer of personal data being processed. This register shows the date of transfer, the legal basis for transfer, the recipient, the scope of personal data transferred and other data required by the law prescribing the obligation of processing.

(2) Personal data may be transferred, data provision may be carried out and different data processing activities may be linked only if the data subject has given consent, or if this is required or permitted by law, and the conditions for data processing are met for each individual piece of personal data.

(3) The data transfer register described above can take the form of a data base or hard copy documents.

(4) The data transfer register must be retained for 5 years.

39. §
Internal processing records

(1) The head of the organisational unit shall send information to the employee responsible for maintaining processing records for the registration of every processing task belonging to the scope of responsibilities and competence of the organisational unit managed by him or her in the internal processing records of the University, using the registry sheet included in Annex 1 and providing the content required therein,

a) 25 days prior to starting the processing, if possible;

b) 25 days prior to starting the processing of a new data set or the use of new technology;

c) when processing is required by law, no later than within 10 days of the announcement of the law, if possible.

(2) The internal processing records are kept by the employee responsible for maintaining the processing records on the basis of the registry sheets received by him or her. Upon request, he or she shall make them available to the supervisory authority.

(3) The processing task is given a registration number which serves as an identification number that must be indicated with every transfer, publishing and disclosure of the data, when the data are handed over to the data subject, a personal data breach is reported or a change in processing is reported.

(4) Changes in any processing listed in the internal processing register must be reported by the head of the organisational unit obliged to report the change without undue delay, through the completion of the relevant fields of the registry sheet, to the employee responsible for keeping processing records who will then make the necessary changes in the records on the basis of the request.

(5) Any ad-hoc data transfer carried out on the basis of requests for any processing included in the internal processing register must be reported by the head of the organisational unit obliged to report the transfer without undue delay, through the completion of the relevant fields of the registry sheet, to the employee responsible for

keeping processing records who will then register the data transfer in the data transfer register of the University on the basis of the report.

(6) The data in the internal processing records must not be deleted.

40. §
Employee register

(1) The employee register is used for processing and documenting facts in connection with the employment relationship of teachers, researchers and other employees. The legal basis for this includes the NHEAct, Act I of 2012 on the Labour Code, Act XXXIII of 1992 on the legal status of civil servants (hereinafter referred to as: "act on civil servants") in the first five years of employment established as a result of a change in the operator of the institute on the basis of Section (6) of Article 117/C of the NHEAct, the executory orders of the aforementioned laws, the Organisational and Operational Rules of the University (in particular, part II. Employment Requirement System (hereinafter referred to as: "ERS")) and the Collective Agreement.

(2) The employee register may be used for establishing facts relating to the employment relationship of teachers, researchers and non-teacher and non-researcher employees, providing statistical data and administration particularly in connection with the following contracts: employment contracts, educational contracts for students, educational contracts for doctoral students, service contracts, contracts of use, contracts for work and services, task-based agreements, invention remuneration agreements and voluntary contracts of public interest where daily fees are paid.

(3) The employee register includes the data of all the employees of the University mentioned in Section (2) above.

(4) The data of the employee register are provided by the data subjects in accordance with the Privacy and Data Protection Policy of the University.

(5) The employee register is managed by the organisational unit responsible for employment-related tasks at the University.

(6) The employee register is managed in electronic form and hard copy. The employees shall be informed of any data handling, processing and data transfer carried out in this system in a privacy notice available to everybody.

(7) The wage and labour-related records are subject to the provisions relevant to the employee register, with the exceptions set forth in Section (8).

(8) The data of the wage and labour-related records may be used for establishing facts in connection with the employment relationships of the employees, verifying compliance with the classification criteria, payroll accounting, social insurance administration and the provision of statistical data.

41. §
Student register

(1) The student register is a data base used for documenting student status information in accordance with the provisions of the law and university regulations. The employee register is managed by the organisational unit responsible for organisation of education at the University. The scope of data being processed is specified in Annex 3 of the NHEAct. Students shall be informed of their data being processed in a privacy notice in accordance with the currently valid version of the NHEAct.

(2) In addition to the employee register set forth in Annex 3 of the NHEAct, the University keeps separate records on student events and the data being processed during the processes specified in the Student Requirement System included in Part III of the Organisational and Operational Rules. The students shall be informed of the data being processed in a privacy notice.

42. §.
Records necessary for the eduID Identity Federation

(1) The University provides central identification services for the operation of its IT services, in particular its mailing, library and e-learning systems, as well as the system belonging to the national identity federation (eduID).

(2) The records necessary for the eduID identity federation are managed by the Directorate of Information Technology.

(3) Within the scope of Section (1) above, the data of the persons having no employment relationship with the University referred to in Section (4) of Article 2 of this Policy and using the library system of the University are managed by the University Library and Knowledge Centre of the University of Pannonia and the Library of the University Center of the University of Pannonia at Zalaegerszeg in connection with and to the extent necessary for their usage of the library system.

43. §

Records kept on the exercise or refusal of the data subjects' rights

(1) The data protection officer of the University keeps records of the requests submitted by the data subjects, as part of exercising their rights, and refused by the University, the measures taken and the reasons for refusal in an electronic form in accordance with Annex 4 (hereinafter referred to as: "register of the data subjects' requests").

(2) The maintenance of the register of the data subjects' request serves the purpose of making the administration of requests submitted by data subjects verifiable, transparent and provable at the University.

(3) The organisational unit responsible for processing shall inform the data protection officer of the refusal of requests submitted to the University by the data subjects, as part of exercising their rights, by sending the document and the reasons within 3 working days of such refusal.

(4) The data protection officer shall maintain a register on the requests refused on a university level and use it for compliance with his or her obligations set forth in Section (3) of Article 16 of the InfoAct.

(5) The organisational units responsible for processing shall start a new register for requests submitted by the data subjects, while the data protection officer shall start a new register for the data subjects' requests being refused on the 1st of each January. The organisational unit responsible for processing shall retain the register of requests submitted by the data subjects in a given year for 2 years, while the data protection officer shall retain the register of requests refused in a given year for 5 years following the current year.

44. §

Register of personal data breaches

(1) The University, through the data protection officer, shall maintain an electronic register on the basis of the reports sent by the head of the organisational unit in charge in accordance with Annex 2 in order to verify the measures taken in connection with the personal data breach and inform the data subjects.

(2) It must be made available to the supervisory authority upon request.

Chapter VIII

PUBLICATION OF DATA OF PUBLIC INTEREST AND THE MANAGEMENT OF REQUESTS TO HAVE ACCESS TO DATA OF PUBLIC INTEREST

45. §

Publication of data of public interest

(1) With respect to matters falling under its scope of duties, including in particular its budget, the management of its assets, the use of public funds and the contracts concluded in connection with this, as well as special and exclusive rights conferred upon market actors, private organisations or individuals, the University shall promote and ensure that the general public is promptly provided with accurate information.

(2) The University's data of public interest and data accessible on public interest grounds must be freely available on the University's website. The scope of data and the organisational units responsible for their maintenance are included in a Chancellor's directive.

46. §

Rules on access to data of public interest

(1) The University shall allow any person to have free access to data of public interest and data accessible on public interest grounds under its control if so requested, with the exceptions provided by the InfoAct.

(2) Anyone can submit a request for access to data of public interest orally, in writing or by electronic means or by filling in the Request Form in Annex 5 and submitting it to the University. Such a request can be submitted to: address: 8200 Veszprém, Egyetem street 10., postal address: Veszprém 8201 Pf. 158, e-mail address: adatvedelem@uni-pannon.hu.

(3) Requests submitted orally must be documented in the relevant records which must include the dates used as significant deadlines. Access to data accessible on public interest grounds shall be governed by the provisions pertaining to access to data of public interest. Requests for access to data of public interest must be submitted to the Chancellor's Office or, if it has been submitted to another organisational unit, it must be immediately forwarded to the Chancellor's Office.

(4) The data protection officer shall immediately verify if the criteria set forth in Sections (1a) and (1b) of Article 29 of the InfoAct are met for the registered request for access to data.

(5) The data protection officer, following the verification process mentioned in Section (4) of Article 46, shall inspect – if necessary, with the involvement of the organisational unit concerned by the data – the request for access to data to see if it is clear and unambiguous and if it relates to data being processed by the University.

(6) Any request for access to data of public interest must be fulfilled as soon as possible but in no way later than 15 days or the request be refused.

(7) If the request concerns data large in number or in volume, or if fulfilling the data request requires a disproportionate use of the labour resources needed for the performance of the core duties of an organ performing public duties, the time limit of 15 days may be extended by 15 days on one occasion, of which the requesting party shall be informed within 15 days of the date of receiving the request.

(8) If the data request is unclear, the Chancellor, based on the information prepared by the data protection officer, calls on the requesting party to clarify the request.

(9) If the requesting party fails to respond to the call for clarification of the data request within 30 days, the request shall be deemed to be withdrawn. Information of

this must be sent to the requesting party when he or she is called on to clarify the request.

(10) Any request for data of public interest being processed by the University, if there is no doubt that the requested data are of public interest, must be fulfilled as soon as possible in a comprehensible form and via the means requested by the requesting party. The competent organisational unit shall be responsible for collecting and preparing the data requested.

(11) If a document containing public-interest data also includes information that the requester is not entitled to access, that information must be rendered unrecognizable on the copy.

(12) If the requesting party wishes to have the data of public interest in a written form, the data protection officer shall submit the draft letter containing the requested data to the Chancellor for approval.

(13) If the requesting party wished to have access to the data by inspecting them or receive the copies of the documents in person, the data protection officer shall contact the requesting party to find an appropriate date for this.

(14) Enough time shall be given for the inspection of the data in a room designated for this purpose. The requesting party's questions shall be answered while inspecting the document handed over to him or her. The requesting party shall have the right to take notes of the document handed over to him or her.

(15) Regardless of how it is stored, the requester may receive a copy of any document or part of a document containing the data. The University may charge a fee for fulfilling the data request – covering the costs incurred – if the costs exceed the minimum amount specified as chargeable in the applicable government decree, provided that the fee determined in this way does not exceed the maximum amount set by the decree. The requester must be informed within 15 days of submission about the amount of the fee and the options for fulfilling the request that do not require copying.

The amount of the fee shall be determined by the organisational unit responsible for fulfilling the data request, and the Chancellor's Office shall communicate it to the requester.

(16) The requesting party shall make a statement within 30 days from receiving the information as to whether he or she wishes to maintain his or her request or not. The period between providing the information and the receipt of the requesting party's

statement shall not be taken into account when calculating the time limit available for the fulfilment of the request. If the requesting party maintains his or her request, he or she shall pay the fee to the University within the time limit determined by the University which is least 15 days.

(17) If fulfilling the data request requires a disproportionate use of the labour resources needed for the performance of the University's core duties, or the document or a part of the document of which the copy had been requested is large, or if the amount of the fee exceeds the amount determined in the relevant government decree, the request shall be fulfilled within 15 days from the date on which the payment of the fee was made by the requesting party.

(18) The fee is determined by the organisational unit concerned by the data request according to the verified costs (calculation of net costs) related to the fulfilment of the request. When determining the amount of the fee, the following cost elements may be taken into account:

a) the cost of the data carrier containing the requested data, and

b) the cost of delivering the data carrier containing the requested data to the requester.

(19) When determining the fee, the organisational unit in question may request information from the Directorate for Economic Affairs in connection with the various cost items.

(20) The method of payment shall be indicated by the requesting party in his or her statement submitted as a response to the information sent him or her about the fee before the fulfilment of his or her data request. The requesting party's attention must be called to this in the information sent in connection with the fee.

(21) The fulfillment of any data request that concerns data not managed by the University, or data that do not qualify as public interest data, or that would require the creation of new data by comparing public interest data or data publicly available for public purposes with data already held by the University, shall be rejected.

(22) The report on public interest data requests shall be made freely accessible on the University's website by the Directorate of Legal Affairs and Procurement at the frequency prescribed by law.

(23) The register must include:

a) the registration number,

b) the filing number,

c) the subject of the request for data of public interest,

d) the data of the request for data of public interest,

e) the name of the organisational unit concerned,

f) the reimbursement of costs (yes/no),

g) the fulfilment of the data request (yes/no),

h) comments

Chapter IX

PROVISIONS GIVING EFFECT TO THIS POLICY

(1) This Policy enters into force on 1st December 2025. This Policy shall be used for the activities of the University of Pannonia in connection with privacy and data protection, from the day it enters into force. The provisions of this Policy shall be used for cases started after this Policy has entered into force.

Chapter X

DEFINITIONS

(1) For the purposes of this Policy, the following definitions apply:

a) data subject: a natural person identified or identifiable based on any information;

b) personal data: any data or information relating to the data subject;

c) sensitive data: all data falling in the special categories of personal data that are personal data revealing racial or ethnic origin, political opinion, religious belief or worldview, or trade union membership, as well as genetic data, biometric data for the

purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

d) biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

e) data concerning health: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the health status of the natural person;

f) criminal personal data: personal data related to the data subject and to a criminal record, generated by organs authorised to conduct criminal proceedings or to detect criminal offences, or by the prison service during or prior to criminal proceedings, in connection with a criminal offence or criminal proceedings;

g) data of public interest: information or data other than personal data, registered through any method or in any form, pertaining to the activities of and processed by the organ or person performing state or local government duties and other public duties defined by law, or generated in the course of performing their public duties, irrespective of the method or form in which it is recorded and regardless of its singular or collective nature; in particular, data concerning material competence, territorial competence, organisational structure, professional activities and the evaluation of their performance, the type of data held and the laws governing its operation, as well as data concerning financial management and concluded contracts;

h) data accessible on public interest grounds: any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by the law for the benefit of the general public;

i) consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

j) objection: the data subject's statement with which he or she objects to the processing of his or her personal data and requests the processing to be stopped or the data being processed to be erased;

k) controller: the natural or legal person or organisation having no legal personality which, alone or jointly with others, determines the purposes and means

of the processing of personal data, makes decisions concerning data processing (including the means used) and implements such decisions or ensures that they are implemented by the processor;

l) processing: any operation or set of operations which is performed on personal data, regardless of the procedure applied; in particular collecting, recording, registering, organising, storing, modifying, using, retrieving, transferring, disclosing, synchronising or connecting, blocking, erasing and destroying the data, as well as preventing their further use; taking photos and making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples and iris scans);

m) data transfer: providing access to the data for a designated third party;

n) disclosure: making the data accessible to anyone;

o) data erasure: making the data unrecognisable in such a way that its restoration is

no longer possible;

p) data identification: attaching an identification string to the data to differentiate it from other data;

q) restriction of processing: the blocking of stored data by marking them with the aim of limiting their processing in the future;

r) data destruction: the complete physical destruction of the data-storage medium that contains the data;

s) technical processing: the performance of technical tasks relating to processing operations, regardless of the method or means used for such operations or of the place of application, provided that the technical tasks are carryout out on the data;

t) processor: a natural or legal person, or an organisation having no legal personality who or which processes personal data on the basis of a contract, including contracts concluded under the conditions laid down in an Act;

u) data source: the organ performing public duties, which generated the data of public interest that is to be published through electronic means, or during the operations of which such data was generated;

v) data publisher: the organ performing public duties which, if the data source itself does not publish the data, uploads the data sent to it by the data source to a website;

w) data set: all data processed in a single register;

x) third party: a natural or legal person or an organisation having no legal personality other than the data subject, the controller or the processor;

y) personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transfer or disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed;

z) pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Chapter XI

TRANSITIONAL AND FINAL PROVISIONS

(1) This Policy was adopted by the Senate at its meeting of 30th October 2025 through its Resolution 169/2025. (X.30.).

(2) This Policy enters into force on 1st December 2025.

(3) Simultaneously to this Policy entering into force, the 'Privacy and Data Protection Policy' adopted by the Senate at its meeting on 26th October 2023 by Resolution No. 200/2023. (X.26.) shall cease to have effect.

(4) Annexes to this Regulation:

Annex 1: Data Processing Registry Sheet
Annex 2: Data Protection Incident Reporting Form
Annex 3: Privacy Notice Template
Annex 4: Registration of requests submitted by data subjects
Annex 5: Request form for access to data of public interest

Dated in Veszprém, on 30th October 2025

Dr. János Abonyi
Rector

Zsolt Csillag
Chancellor

On behalf of the Foundation for the University of Pannonia, acting as Operator, approved by:

Dated in Veszprém, on 30th October 2025

Dr. Péter Bartus
Executive Director