INTERNAL DATA PROTECTION POLICY

OF THE

UNIVERSITY OF DEBRECEN

Effective from 24 September 2021

Table of Contents

THE PURPOSE OF THE POLICY....5
CHAPTER I....5
THE SCOPE OF THE POLICY; DEFINITIONS....5
The substantive scope of the Policy....5
The personal scope of the Policy....5
Definitions of terms....6
CHAPTER II....10
THE FUNDAMENTAL REQUIREMENTS OF THE LAWFULNESS OF DATA PROCESSING....10
The basic principles of the data processing....10
The requirements of the application of consent as the legal basis....11
The requirements of the application of contractual relationship as the legal basis....12
The requirements of the application of legal obligation as the legal basis....13
The requirements of the application of force majeure as the legal basis....13
The requirements of the application of legitimate interest as the legal basis....13
The processing of sensitive data....14
The obligation to provide information in advance....15
CHAPTER III....16
REQUIREMENTS APPLICABLE TO THE PROCESSING OF DATA BY THE UNIVERSITY....16
Records of processing activities....16
Rules of procedure applicable to drawing up the Policy....16
Requirements related to the processing of students' personal data....17
Student records....17
The basic requirements applicable to the processing of the personal data of employees....20
Remuneration and employment records....21
The personal and sensitive data recorded and processed by the institutes of public education maintained by the University....21
The personal and sensitive data recorded and processed by the child welfare institutes maintained by the University....22
CHAPTER IV....22
THE EXERCISE OF RIGHTS BY DATA SUBJECTS....22
The division of tasks during the exercise of rights by data subjects....22
Right of access....22
The right to receive a copy of the data....23
Right of rectification....24

Right to erasure 24
Right to be forgotten 25
The right to restrict the processing 25
Right to data portability 26
The right of objection 27
The identification of the data subject 27
Deadline for compliance with the request 28
Compliance with the data subject's request 28
Refusal of the data subject's request 29
CHAPTER V 30
FUNDAMENTAL DATA SECURITY MEASURES 30
IT security measures 30
Organisational security measures 31
CHAPTER VI 32
THE HANDLING AND REPORTING OF PERSONAL DATA BREACHES 32
The handling of personal data breaches 32
Finding out about a personal data breach 32
The suspension of the processing in case of a personal data breach 33
The reporting and investigation of the personal data breach 34
Dispensing with the reporting of the personal data breach 35
Informing the data subjects 36
Written record of the investigation and the record of personal data breaches 37
CHAPTER VII 38
THE DATA PROTECTION OFFICER AND THE DATA SECURITY CENTRE 38
Provisions applicable to the Data Protection Officer 38
Cooperation with the supervisory authority 40
Data Protection Centre 41
Area Data Protection Officer 41
CHAPTER VIII 42
FURTHER OBLIGATIONS RELATED TO DATA PROCESSING 42
The use of processors 42
Data protection impact assessment 43
Joint processing 44
CHAPTER IX 44

RESPONSIBILITY FOR COMPLIANCE WITH THE RULES OF DATA PROCESSING, CONTROLS 44
CHAPTER X 45
DATA TRANSMISSION 45
Data transmission 45
Obligations related to data transmissions to third countries 46
Records of data transmissions 47
CHAPTER XI 48
Electronic surveillance system 48
CHAPTER XII 48
MISCELLANEOUS AND CLOSING PROVISIONS 48
ANNEXES 50
Annex 1 50
Annex 2 54
Annex 3 56
Annex 4 60
Annex 5 61
Annex 6 62
Annex 7 64
Annex 8 65
Annex 9 66
Annex 10 67
Annex 11 68
Annex 12 71
Annex 13 76
Annex 14 ..... **Hiba! A könyvjelző nem létezik.**

The Senate of the University of Debrecen, in order to ensure that the processing of the data of its staff, students and other data subjects is performed lawfully and fairly, as well as in a manner that is transparent for all, pursuant to Regulation 2016/679/EU on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC (hereinafter: the General Data Protection Regulation of the European Union or GDPR), Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: the Information Act), Act CCIV of 2011 on National Higher Education

(hereinafter: the National Higher Education Act), Act I of 2012 on the Labour Code (hereinafter: the Labour Code), Government Decree 87/2015 (IV.9.) on the Implementation of Certain Provisions of the Act on National Higher Education Act (IV. 9 (hereinafter: Implementing Decree), Government Decree 423/2012 (XII.29.) on the Admission Procedure to Higher Education (XII. 29 (hereinafter: the Admissions Decree), Act LXXVII of 2013 on Adult Education (hereinafter: Adult Education Act), Act CXC of 2011 on National Public Education, the provisions of law pertaining to child welfare institutions, the continued education of teachers, as well as other relevant provisions of law, in harmony with the applicable rules of the University, hereby adopts the following internal policy (hereinafter: Policy), in which it shall present how it complies with the obligations arising from the relevant provisions of law and applicable to its activities.

THE PURPOSE OF THE POLICY

The purpose of the Policy is to ensure at the University of Debrecen (hereinafter: University) that the keeping of data processing records, the processing and protection of data take place in line with the relevant provisions of law, in a safe manner, and in compliance with the European Union's General Data Protection Regulation (GDPR).

CHAPTER I

THE SCOPE OF THE POLICY; DEFINITIONS

The substantive scope of the Policy
Section 1

(1) The Policy shall be applicable to all data processing by the University, whether such processing pertains to employees or persons performing work at the University in other statuses, students or other data subjects.

(2) The special rules applicable to health-related records and data processing shall be determined by the University in a separate policy, on the basis of the present Policy and other provisions of laws applicable to the processing of data concerning health, which is available at https://mad-hatter.it.unideb.hu/portal/displayDocument/id/2355067.

The personal scope of the Policy
Section 2

(1) The personal scope of the present Policy shall cover the following:

a) students of the University, regardless of the form of education;
b) children participating in kindergarten education, school education or receiving day-care services provided by institutes of public education maintained by the University, as well as the legal guardians of such children;
c) persons not having the status specified in point a) above, applying for or undergoing a habilitation procedure, as well as persons having the legal status of doctoral candidates;
d) all persons in the employment of the University, regardless of the specific type of legal relationship through which they work (including persons working under retainers, service contracts or under legal relationships);
e) persons not having the status specified in point a) or d), participating in adult education courses organised or administered by the University (hereinafter collectively: adult education), in-service training for teachers, those applying for and participating in doctoral degree awarding procedures, as well as persons using the library system of the University;
f) all organisational units of the University engaged in data processing;
g) persons possessing certain titles (e.g. *professor emeritus, professor emerita, doctor honoris causa*); and
h) persons who are not in a legal relationship with the University, but whose data the University processes or is required to process pursuant to a provision of law, for the purpose of establishing a legal relationship, as well as persons who participate in the data processing activities of the University under any legal title, also including secondary school students participating in academic activities.

Definitions of terms
Section 3

(1) Data subject: a natural person identified or identifiable on the basis of any information. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors.

(2) Personal data: any information pertaining to an identified or identifiable natural person.

(3) Sensitive data: pursuant to the present Policy, sensitive data shall primarily include data concerning health. Sensitive data shall also include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, as well as data concerning a natural person's sex life or sexual orientation.

(4) 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 his or her health status.

(5) Contact persons of business partners: natural persons who make available to the University their personal data in their capacity as representatives of a legal person or other organisation. The provisions pertaining to the contact persons of business persons shall also be duly applicable to sole traders.

(6) Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(7) Anonymisation: such processing of personal data as a result of which it can no longer be determined without the use of further information who the specific natural person is that the personal data refers to, provided that such further information is stored separately, and it is ensured by way of technical and organisational measures that the personal data cannot be linked to identified or identifiable natural persons.

(8) Transmission: the making of data accessible to a specific third party.

(9) Disclosure: the making of data accessible to anyone.

(10) Erasure: the making of data unrecognisable in a way that it can never again be restored.

(11) Restriction of processing: the marking of stored personal data with the aim of limiting their processing in the future.

(12) Destruction: the physical destruction of the medium containing the personal data.

(13) Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(14) Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

(15) Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

(16) Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

(17) Consent: the 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.

(18) Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(19) Trade secret: any fact, information and other data, or a compilation thereof, connected to the economic activities of the University, which are not publicly known or which are not easily accessible to other operators pursuing the same economic activities, and which, if obtained and/or used by unauthorized persons, or if published or disclosed to others are likely to imperil or jeopardize the rightful financial, economic or commercial interest of the University, provided that the party rightfully disposing over such trade secrets shall not be imputable in connection with the preservation of the same. Protection identical with trade secrets shall also apply to technical, economic and other practical knowledge of value held in a form enabling identification, including accumulated skills and experience and any combination thereof ("know-how").

(20) Bank secret: any fact, piece of information, solution or data item that relates to the identity, data, financial position, business activity, management, or ownership and business relations of the University, or to the balance and movements of its bank account managed by a financial institution or its contracts concluded with a financial institution.

(21) GDPR: Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation of the European Union). The acronym GDPR, widely used in practice is derived from the English name of the regulation (General Data Protection Regulation).

(22) Applicable law: the GDPR, as well as the opinions, guidelines of the Article 29 Working Party on Data Protection, the documents of the European Data Protection Board, as well as the Hungarian provisions of law adopted on the basis of or with a view to the authorisation provided by the GDPR, other provisions of law in the field of data protection, the document issued by the National Authority for Data Protection and Freedom of Information (hereinafter: NAIH), and the codes of conduct applicable to the University, the controller or the processor.

(23) EEA state: A member state of the European Union or a state which is party to the agreement on the European Economic Area; further, a state whose citizens have the same legal status as citizens of the European Union and its member states and a state that is not a party to the agreement on the European Economic Area but has an international agreement pursuant to which its citizens have the same legal status as citizens of a state which is party to the agreement on the European Economic Area.

(24) Third country: All states that are not EEA states as defined above.

(25) Data Protection Officer: a person having the necessary knowledge of the legal requirements pertaining to the protection of personal data and experience in the field of the application of the law, appointed by the chancellor of the University, who is capable of the performance of the tasks specified in Section 25/M (1) of the Information Act.

(26) Legal representative: an attorney-at-law, European Community lawyer, foreign legal advisor, chamber counsel, associate attorney, associate European Community lawyer, articled clerk or legal clerk entered in the registry of a bar association, retained by the University, who may act on behalf of the University in cases of data protection, or participate in the resolution of such cases.

(27) Data protection*:* such procedures collectively the aim of which is the protection of the personal data of natural persons.

(28) Data security: its subject is data itself, which means the protection of the confidentiality of the data; it is created by way of technical and organisational measures.

(29) Private-purpose use: the use of personal data for all such purposes that occurs in the absence of a legal basis specified in the present Policy.

(30) Organizational unit: The organisational units of education and research, service provision and administration, the various functional organisational units, and the Student Government, which are listed in "The organization of the University" section of the Rules of Organization and Operation of the University of Debrecen.

(31) Legal basis: the group of cases, as defined by law, where the processing of the personal data is lawful.

CHAPTER II

THE FUNDAMENTAL REQUIREMENTS OF THE LAWFULNESS OF DATA PROCESSING

The basic principles of the data processing
Section 4

(1) If the University determines the circumstances and manner of data processing, then such processing shall comply with the basic principles set forth in the GDPR and the requirements of the present Policy.

(2) Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

(3) The University shall design and implement the data processing in such a way that it should be lawful and fair, as well as transparent to all data subjects (principle of lawfulness, fairness and transparency). The University shall have an appropriate legal basis for the processing of personal data. The University may only process personal data if it has the legal basis according to Article 6, 8 or 9 of the GDPR, and in case the requirements prescribed by the relevant provisions of applicable law in connection with the application of the legal basis are satisfied. The University may keep records of such data that are indispensable, pursuant to Article 6(1)(e) of the GDPR, for the performance of a task carried out in the public interest, for its proper operation, for the exercise of the employer's rights, for the organization of the educational activities, etc., and further, which are necessary for making decisions on and certifying the right to any allowances or benefits under the relevant provisions of law and in the rules of organization and operation.

(4) In the course of processing data, the University shall ensure that data are only collected for clearly specified and lawful purposes. The purpose of the data processing shall be express, clearly defined and lawful, and further, it shall be determined already at the time when the data processing is commenced. Personal data may not be processed in a manner that is not reconcilable with the original purposes of the processing (the principle of purpose limitation).

(5) The University shall design and implement the data processing in such a way that the data processed are suitable and relevant for the purposes of the data processing, and their processing is restricted to the necessary extent. The University shall ensure, in particular, that the period for which personal data are stored is limited to a strict minimum. In the interest of the above, the University shall establish time limits after which the data are deleted, aligned with the purposes of the data processing and the relevant requirements of the law (the principle of data minimisation, storage limitation).

(6) The University shall ensure that the data processed are accurate and, if necessary, up to date (the principle of accuracy).

(7) The University shall design and implement the data processing in such a way that personal data are stored to ensure that it makes the identification of the data subjects possible only for the duration of time necessary for achieving the objectives of the data processing (principle of storage limitation).

(8) When designing its data processing, the University shall take into consideration that, by way of using suitable technical or organisational measures, the appropriate security of the personal data shall be ensured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (the principle of integrity and confidentiality).

(9) The University shall be responsible for ensuring that the data processing should satisfy the requirements of Article 5 (1) of the GDPR. The University shall be capable of certifying that its data processing is in compliance with Article 5 (1) of the GDPR. All employees of the University, as well as the data controllers and processors in a contractual relationship with the University shall be subject to an obligation to cooperate in the interest of performing the above (the principle of accountability).

The requirements of the application of consent as the legal basis
Section 5

(1) The University may only use consent as a legal basis if all requirements prescribed by the present Policy and the applicable law are satisfied.

(2) The University shall be able to demonstrate that the data subject has consented to processing of his or her personal data. The University shall primarily satisfy this obligation through electronic logging or by way of retaining the written consent given by the data subject.

(3) In the course of the processing, the University shall ensure that the data are only processed if the data subject gives his or her consent by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of agreement to the processing of the personal data, such as by a written statement, including by electronic means, or an oral statement. If the University asks for the data subject's consent via its website, it shall be done with the use of suitable IT solutions (e.g. by way of placing a checkbox on the web page through which the consent of the data subject can be obtained).

(4) Consequently, a tacit agreement, using pre-ticked boxes or the lack of activity shall not constitute consent.

(5) In the course of designing and implementing the data processing, the University shall ensure that the data subject may consent to processing separately for each purpose of data processing .

(6) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the University shall ensure that the request for consent be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. On its electronic or paper-based forms, the University shall ensure that the parts of the text asking for consent are separated from the rest of the form.

(7) The consent of the data subject shall be voluntary, and in order to ensure the above, the University shall take into account that:

a) it may not make the performance of a contract conditional on whether the data subject consents to processing that is not necessary for the performance of the contract;
b) the data subject shall have actual and free choice in giving his/her consent, and shall have an opportunity to refuse or revoke his/her consent without any adverse effect;
c) there shall be no uneven relationship between the University and the data subject which would render it unlikely that the consent concerned was given voluntarily.

(8) The University shall ensure that it is as easy to withdraw the consent as it is to grant it.

(9) In case of processing of data related to its employees, the University may only use consent as the legal basis in exceptional cases, when the above requirements are fulfilled.

(10) The consent of the data subject shall be considered as given with respect to personal data disclosed or published by the data subject in the course of his/her public appearances.

(11) In case of doubt it shall be presumed that the consent of the data subject is not given.

The requirements of the application of contractual relationship as the legal basis

Section 6

(1) The University may only use contracts as the legal basis if all requirements prescribed by the present Policy and the applicable law are satisfied.

(2) When using a contractual relationship as the legal basis, the University needs to prove that:
   a) the processing of the personal data is necessary for the performance of a contract concluded with the data subject;
   b) the processing of the personal data is necessary prior to the conclusion of the contract for the steps requested by the data subject.

The requirements of the application of legal obligation as the legal basis
Section 7

(1) The University may only use legal obligation as the legal basis if all requirements prescribed by the present Policy and the applicable law are satisfied.

(2) For the application of legal obligation as the legal basis, the University shall specify the EU or Hungarian legislation that prescribes or necessitates the processing of the personal data.

(3) Where the law determines the circumstances of the processing, the University shall not process the data for any other purpose or different duration, and may not extend the processing to other personal data.

(4) If the provision of law determining the legal obligation does note regulate the purpose or duration of the processing, the scope of the personal data processed, or the conditions of the processing, these shall be determined University with attention to the principles in Section 4 of this Policy and in compliance with the relevant requirements of the applicable law.

The requirements of the application of force majeure as the legal basis
Section 8

(1) All citizens of the University shall have the right to process personal data to the extent necessary for the protection of the vital interests of the data subject. (Such cases include, for example, when it is necessary to call an ambulance for a data subject, and in the course of the call, the personal and health data of the data subject must be communicated.)

(2) If any employee of the University transmits personal data with the application of force majeure as the legal basis, but the data subject or another person contests the lawfulness of such transmission, the University shall participate in the clarification of the circumstances of the data transmission.

The requirements of the application of legitimate interest as the legal basis
Section 9

(1) The University may only use legitimate interest as the legal basis if all requirements prescribed by the present Policy and the applicable law are satisfied, and the requirements prescribed in connection with the balancing of legitimate interest are satisfied.

(2) The legitimate interests of the University or of third parties shall be actual, unambiguous and lawful. The University shall strive to ensure that, wherever possible, a written document (e.g. contract, NAIH opinion, resolution, decision of the data protection authority of another EU member state) be available to prove legitimate interest.

(3) When determining legitimate interest, the University shall examine, among other things, if the data subject may reasonably expect at the time when the personal data are collected, and in connection with such collection of personal data, that their processing may take place for the given purpose. It may be a legitimate interest, for example, when a relevant and appropriate connection exists between the data subject and the University, for example, in cases where the data subject is a citizen of the University.

(4) For the application of legitimate interest as a legal basis, the University shall be required to demonstrate the legitimate interests and expectations of the data subjects by way of preparing a balancing test. As far as possible, the University shall obtain the opinions of the data subjects or their representatives on the proposed data processing. If the University fails to demonstrate the interests of the data subjects, the processing shall not be permitted.

(5) In order to ensure that data processing by the University with the application of balancing tests should not restrict the rights and freedoms of data subjects in a disproportionate way, the University shall introduce appropriate safeguards. As far as possible, the University shall obtain the opinions of the data subjects or their representatives on the proposed safeguards. If the University fails to demonstrate the appropriate safeguards, the processing shall not be permitted.

(6) If an organisational unit of the University wishes to use the legal basis of legitimate Interest, it shall be required to demonstrate, by way of using the questionnaire in Annex 1 attached to the present Policy, the lawfulness of the proposed processing, and shall be required to carry out a balancing test (Annex 2).

The processing of sensitive data
Section 10

(1) The University may process sensitive data if a provision of law specifically requires the processing of sensitive data, or where the processing of such data is clearly necessary for the performance of a legal obligation.

(2) The University may process sensitive data on the basis of the express consent of the data subject if the data subject gives such consent to the University in the interest of exercising a right of the data subject. It should be clear from the declarations, communications of the data subject that he/she is aware what right it is in the interest of the exercise of which the consent is given.

(3) If the processing of sensitive data is necessary for the establishment, exercise or defence of legal claims, the University shall document why the processing (use, transmission) of the sensitive data is necessary. It may also be accepted as such documentation if, in a document prepared in the course of the procedure, the University expressly discusses the necessity of the processing (use, transmission) of the sensitive data.

The obligation to provide information in advance
Section 11

(1) The University shall inform the data subjects of all processing of data. If the University fails to inform the data subjects of the processing of their data in advance, the processing shall not be permitted.

(2) The University shall perform its obligation to inform the data subjects by way of drawing up and publishing or providing privacy (data processing) policies. All organisational units shall draw up data processing policies with respect to their own areas of activity (Annex 3). In case of the performance of significantly complex tasks, the head of an organisational unit may decide to draw up several privacy policies. Exceptionally, it is also acceptable if the University provides case-by-case information to the data subjects in connection with particular instances of data processing.

(3) If the University obtains the personal data directly from the data subject, the privacy policy shall cover the following circumstances of data processing:

a) the name and the central e-mail address of the University, the name of the given organisational unit, as well as the name and contact information of its representative;
b) the designation of the given processing activity, its objective, the scope of the data processed, the legal basis, the duration for which the data are retained, or in case this is not possible, the criteria used in determining this duration;
c) in case of application of legitimate interest as the legal basis, the legitimate interests of the University or third parties;
d) the recipients or categories of recipients of the personal data;
e) information on the rights of the data subject and the possibility of contacting NAIH;

f) the consent, together with information on the right to withdraw such consent at any time, as well as information to the effect that the revoking of the consent shall not affect the processing of data based on consent before such revocation;
g) whether the provision of personal data is a statutory obligation or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

(4) If the University obtains the personal data not directly from the data subject, the privacy policy shall state what source the personal data were obtained from.

(5) The privacy policy shall be transparent. The policy shall be divided into paragraphs, and where possible lists shall be used in order to improve the clarity and readability of the text.

(6) The privacy policy shall be made available in an easily accessible form.

(7) The text of the privacy policy shall be written in an accessible, easily comprehensible way. Verbatim quotations of passages from the law shall be avoided in the policy, and an effort shall be made to ensure simple and clear phrasing.

CHAPTER III

The REQUIREMENTS APPLICABLE TO THE PROCESSING OF DATA BY THE UNIVERSITY

Records of processing activities
Section 12

(1) Each organisational unit shall maintain records of the data processing activities performed in its area of responsibility.

(2) The elements of the records shall be as listed in Annex 4.

(3) The data processing records shall be sent to by the organisational units of the University to the Data Protection Centre.

Rules of procedure applicable to drawing up the Policy
Section 13

(1) Organisational units of the University shall send the proposed version of their privacy policies to the Data Protection Centre of the University. The Data

Protection Centre shall review the proposed policy with attention to compliance with the applicable law, the present Policy and other internal policies and orders. After this review, the privacy policy is published in the locally customary and generally known manner, or in the website. The University shall also make the privacy policies of the individual organisational units available on its own website, under the title "Privacy policy".

Requirements related to the processing of students' personal data

Section 14

(1) Pursuant to Section I/B of Annex 3 to Act CCIV of 2011 on National Higher Education (hereinafter: the National Higher Education Act), the University shall process personal data in connection with admission.

(2) After the establishment of the student status, the University shall process the personal data in accordance with point I/B of Annex 3 to the National Higher Education Act.

(3) The University shall retain the personal data for a period of eighty years after the termination of the student status.

Student records

Section 15

(1) The keeping of student records shall be a data processing activity with an aim to document the facts pertaining to student status, the legal basis of which is provided by the National Higher Education Act, the Implementing Decree of the National Higher Education Act, as well as the Rules of Organization and Operation, the Regulations on Student Fees and Benefits, the Academic and Examinations Regulations, the Doctoral Regulations, and other relevant regulations of the University.

(2) The University shall operate a single, integrated IT system, the Neptun Uniform Academic System, for the purposes of maintaining the student records.

(3) The data of the student records may be used for activities related to the performance of the students' academic and examination requirements, the determination and payment of stipends, cost reimbursements, fees, etc., and all other organisational and administrative tasks related to the student status.

(4) The university-level coordination of the Neptun Uniform Academic System, as well as the alignment of the work of the organisations participating in the operation, development and maintenance of the system shall be provided by the Centre of Student Relations and Services.

(5) The source of the data for the student records shall be the admissions database, as well as the enrolment forms completed by the students. The data of the persons involved in the performance of the educational and administrative tasks shall be uploaded to the system by the organizational units, based on their own records. The source of the data included in the database may only be electronically produced or paper-based documents. No information may be entered into the database on the basis of verbal communication.

(6) The method of data entry:

The data recorded in the database shall be the same as included in the document serving as the source. The person entering the data shall be responsible for such correspondence between the data.

If some data in the document serving as the source is impossible to interpret, illegible, inconsistent or incomplete, it may not be entered in the database. In such a case the correction or supplementation of the document serving as the source of the data shall be requested from the data subject, or in case the data is not from the data subject, from the issuer of the document.

(7) The controller of the student's data shall be the employee at the registrar's office of the faculty (or faculties), or at the department, in the framework of which the student studies. The data related to the student may also be processed in the Neptun system by the Centre of Student Relations and Services (HKSZK) – and specifically within the above by the Inter-University Centre for Telecommunications and Informatics (ETIK), the Student Administration Centre (HAK), the Dormitory, the Centre for Mental Health and Equal Opportunities (DEMEK) – as well as the Coordinating Centre for International Education (NOKK), the International Office, and the Doctoral Councils, in each case in accordance with their scope of rights and tasks, as assigned to their roles.

(8) The data in the Neptun Uniform Academic System shall be protected against any unlawful access, alteration, transmission, disclosure, erasure or destruction or accidental destruction or deterioration. Ensuring this protection shall be the task of the operator of the system, the IT Service Centre (ISZK), the Centre of Student Relations and Services (HKSZK), as well as the persons and organisational units responsible for the processing and processing of the data.

(9) In the interest of the security of the data stored on the servers, the IT Service Centre, the unit operating the system, shall institute the following measures and keep them at a high level at all times:

a) keeping the servers in a closed room, with appropriate physical protection; ensuring the environmental and technical conditions for the operation of the servers;

b) making daily security back-up copies from the active data in the databases containing the personal data; the back-up copies and the live database shall be kept on devices located at different campuses or locations;

c) ensuring that the servers on which the personal data are located cannot be reached via direct network access, and hacking into the system is not possible via network access;

d) ensuring that in case of power failures the servers can be shut down in an orderly way, without loss of data;

e) providing for virus protection of the servers;

f) if the database server is accessed via terminal servers, providing for the allocation and the withdrawal of login names and passwords necessary for logging into the terminal servers, as well as for setting up the minimum level of privileges suitable for the purposes of the processing;

g) the system administrator's password to the server and the IT system shall be kept in a fireproof metal case, and the passwords shall be changed at least every six months.

(10) The Neptun Uniform Academic System shall allow the logging of the fact, the date and time of any changes in the data, as well as the person making such changes. The Centre of Student Relations and Services shall set up the system in such a way that logging is enabled.

(11) The maintaining of the student data in the dormitories: In addition to the data stored in the integrated IT system of the University of Debrecen, the dormitory admissions database, as well as the data contained in the enrolment forms completed by the students constitute the basis of the dormitory student records. The data in the records may be used for the purposes of the organizational and administrative tasks related to the status of the students as dormitory residents. The operation and maintenance of the dormitory records system, as well as the processing of the data in that system in accordance with the Internal Data Protection Policy of the University of Debrecen shall be the responsibility of the University Dormitories Directorate of the Centre of Student Relations and Services, with coordination provided by the area Data Protection Officer.

(12) The maintaining of the student data in the dormitory admissions and regular need-based scholarship system: The dormitory admissions and the regular need-based stipend-awarding procedures are conducted by the Dormitory Admissions and Social Committee (KFSZB) operating on the basis of the National Higher Education Act, in accordance with the relevant provisions of law in effect. The scope of personal data requested for the applications on the basis of the relevant provisions of law shall be determined by the Regulations on Student Fees and

Benefits, approved by the Senate.

The basic requirements applicable to the processing of the personal data of employees

Section 16

(1) The University shall process the employee data specified in Annex 3 to the National Higher Education Act.

(2) The institutes of higher education may only process the personal and sensitive data in connection with employment-related issues, the determination and performance of benefits, allowances and obligations, as well as for reasons related to national security, for the purpose of maintaining the records specified in this act, to the extent corresponding to the objectives.

(3) The controller of the data specified in Subsection (1) is the HR Management Directorate; in case of those over the rector exercises the employer's rights, the HR Policy Directorate of the Chancellor's Cabinet; and further, the persons designated by the one exercising the employer's right at the individual organisational units.

(4) The University shall retain the personal data after the termination of employment, for the period specified in the documents archiving policy.

(5) In the interest of the security of the data stored on the system, the IT Service Centre, the unit operating the system, shall institute the following measures and keep them at a high level at all times:

a) keeping the servers in a closed room, with appropriate physical protection. Ensuring the environmental and technical conditions for the operation of the servers;

b) making daily security back-up copies from the active data in the databases containing the personal data; the back-up copies and the live database shall be kept on devices located at different campuses or locations;

c) ensuring that the servers on which the personal data are located cannot be reached via direct network access, and hacking into the system is not possible via network access;

d) ensuring that in case of power failures the servers can be shut down in an orderly way, without loss of data;

e) providing for virus protection of the servers;

f) if the database server is accessed via terminal servers, providing for the allocation and the withdrawal of login names and passwords necessary for logging into the terminal servers, as well as for setting up the minimum level of privileges suitable for the purposes of the processing;

g) the system administrator's password to the server and the IT system shall be kept in a fireproof metal case, and the passwords shall be changed at least every six months.

Remuneration and employment records
Section 17

(1) The keeping of remuneration and employment records shall be a data processing activity with an aim to document the facts pertaining to employee status, as well as other legal relationship aimed at the performance of work, the legal basis of which is provided by the National Higher Education Act, the Labour Code, as well as the Rules of Organization and Operation and the Collective Bargaining Agreement of the University.

(2) The data in the remuneration and employment records may be used for the purposes of establishing facts related to the status of a person as an employee or a person working in another legal relationship aimed at the performance of work, for certifying the satisfaction of the requirements for his/her position, for payroll accounting, social security administration and statistical data supply.

(3) The units managing the records shall be the HR Management Directorate.

(4) The records shall be managed on computers. The security of the data shall be provided for by the controller.

(5) Any supply of data from the remuneration and employment records within the organisation of the University shall be permitted for the rector, the chancellor, as well as for the heads of the organisational units and administrators of such units competent in HR-related issues where the employee works, and for administrators of organisational units who need to have access to a certain group of personal data to perform their tasks.

The personal and sensitive data recorded and processed by the institutes of public education maintained by the University
Section 18

(1) Pursuant to Section 41 of Act CXC of 2011, institutes of public education maintained by the University shall be required to maintain the records prescribed

by law, to log into the information system of public education, as well as to supply summarized data required in the framework of the national statistical data collection programme, as well as on students at the risk of dropping out.

The personal and sensitive data recorded and processed by the child welfare institutes maintained by the University
Section 19

(1) Pursuant to Section 1 of Government Decree 235/1997 (XII.17) on the personal data processed by the guardianship authorities, the regional child protection professional services, the child welfare services and bodies and persons offering individual care, guardianship authorities, bodies and persons offering individual child welfare basic care, and regional child protection professional services are required to maintain the records specified in Annex 1 to the Government Decree. The Child Protection Act contains further, detailed rules concerning the processing of data.

CHAPTER IV

THE EXERCISE OF RIGHTS BY DATA SUBJECTS

The division of tasks during the exercise of rights by data subjects
Section 20

(1) If any organisational unit of the University receives a request for the exercise of a right of a data subject related to data processing or data protection, the head of the given organisational unit shall notify the Data Protection Officer of the request and the answer to be sent to the data subject.

(2) In case of a request sent to the Data Protection Officer, in the interest of replying to the request, the officer shall contact the head of the organisational unit concerned, and shall participate in replying to such request.

Right of access
Section 21

(1) If the data subject exercises his/her right of access (or requests information on the processing of his/her personal data), the University shall provide information concerning the following:

a) what personal data data of the data subject is processed; in this case, it is not sufficient to indicate the category of the data, but the specific personal data need to be identified;
b) what type of processing takes place with respect to the data subject, and what are the purposes and legal bases for the processing;
c) the duration of the processing and the criteria for the determination of such duration;
d) to whom the University transmits the personal data;
e) the rights of data subjects in connection with the processing of their data;
f) if the personal data was not received from the data subject, the source of such data;
g) the right to lodge a complaint with NAIH;

The right to receive a copy of the data
Section 22

(1) If the request of the data subject is specifically aimed at receiving a copy of his/her personal data or the document containing his/her personal data, the University shall make available to the data subject a copy of such personal data.

(2) For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(3) If the data subject requests a copy of camera recordings within the statutory time limit, the possibility of viewing the camera recordings shall be offered to the data subject. In the interest of the above, an appointment shall be agreed upon with the data subject by way of telephone or e-mail. If the data subject uses the possibility of viewing the recording, a written protocol of this fact shall be drawn up.

(4) If the data subject does not used the possibility of viewing the recording or, in addition to the viewing, requests a copy of the recording as well, the University may only issue such recording if the data subject can indicate on what day, at what hour, and approximately at what minute the recording pertaining to him/her was made; and
a) only the data subject is visible on the recording; or
b) in case other persons are also visible on the recording, a processor hired by the University anonymises the recording (makes the image of other persons shown on the recording unrecognizable).

(5) In case of Subsection (4), point b), the University shall charge the cost for the anonymisation, based on an administration fee. The data subject shall be

informed about this amount. The request of the data subject may only be performed if the data subject has paid the amount concerned.

(6) In case of Subsection (5), point b), the University shall lock the recording from the time of the receipt of the application of the data subject, by way of copying to an electronic medium. Such locking shall remain in place until the anonymisation of the recording in accordance with Subsection (5) has taken place, or when the data subject declares that he/she is not willing to pay for the costs of the anonymisation. If the data subject fails to declare within 90 days whether he/she is willing to pay for the costs of the anonymisation, the University shall delete the locked recordings.

Right of rectification
Section 23

(1) The data subject may request that the University rectify (correct) any inaccurate personal information related to him/her.

(2) The request of the data subject may be complied with, if he/she indicated in the request what personal data need to be changed and what are his/her correct personal data.

Right to erasure
Section 24

(1) The University shall erase the personal data if:
   a) the purpose of the data processing ended;
   b) the data subject has withdrawn his/her consent, and the data processing has no other legal basis;
   c) the data subject objects to the data processing, and there are no overriding legitimate grounds for the data processing;
   d) the unlawful processing of the personal data was established by NAIH or the court;
   e) the personal data have to be erased for compliance with a legal obligation in the EU or Hungarian law to which the University is subject;

(2) The University may refuse the data subject's request for the deletion of the personal data, if the University can provide that the processing is necessary:
   a) for exercising the right of freedom of expression and information;
   b) for compliance with a legal obligation which requires the data processing by EU or Hungarian law to which the University is subject;
   c) for the establishment, exercise or defence of legal claims (including, for example, for pressing charges in a criminal case or filing a lawsuit in a civil case).

Right to be forgotten
Section 25

(1) If the University has made the personal data public and is obliged pursuant to the internal privacy policy to erase the personal data, it shall, with attention to the available technology and the cost of implementation, take reasonable steps, including technical measures, to inform controllers that are processing the personal data the links to which the data subject has requested the erasure of, as well as copies or replications of such personal data.

(2) For the exercise of the right to be forgotten, it is necessary for the data subject to indicate what personal data of the data subject was published. If the data subject failed to indicate this in his/her request, the University shall contact the data subject in order to clarify which of his/her personal data the University published.

(3) If the University disclosed the personal data on its own website, it shall be removed from there.

(4) If the personal data published by the University was also published by other controllers, then these other controllers shall also be notified that the personal data shall be deleted.

(5) Using Google's search service, the University shall search for the personal data identified by the data subject to determine if Google lists the personal data concerned in connection with the data processing activity of the University. If so, the removal of the personal data specified by the data subject shall be used via the reporting interface of the Google search engine ("Remove information from Google").

(6) The exceptions shown under "Right of erasure" in this internal privacy policy shall also be applicable when exercising the right to be forgotten.

The right to restrict the processing
Section 26

(1) If the data subject contests the accuracy of the personal data, the University shall restrict the processing until the University checks the accuracy of the personal data. In such a case, the University shall:

a) in case of electronically stored data of contested accuracy, restrict access to such data;
b) in case of documents stored on paper, store the document containing the contested data separately from the other documents, in a sealed envelope.

If the request of the data subject is well-founded, the University shall correct the inaccurate data.

(2) If the processing is unlawful and the data subject opposes the erasure of the personal data, the data subject may request the restriction of the use of such personal data instead. In such a case, the University shall:

a) in case of personal data stored electronically, save the data to an external storage medium (such as a USB flash drive or disc), and delete the electronically stored data from the IT system;
b) in case of documents stored on paper, store the document containing the personal data identified by the data subject separately from the other documents, in a sealed envelope, and hand it over to the data subject in such a way that no copy or duplicate remains in possession of the University.

In his/her request, the data subject shall indicate until what date he/she requests the restriction. If the data subject did not identify this date in his/her request, the University shall ask him/her via e-mail – or in case an e-mail address is not available, via postal mail – to specify until what time he/she requests the restriction.

(3) The data subject may request the restriction of the processing if the University no longer needs the personal data, but the data subject requires the same for submitting, enforcing or defending a legal claim. In such a case, the University shall:

a) in case of personal data stored electronically, save the data to an external storage medium (such as a USB flash drive or disc), and delete the electronically stored data from the IT system;
b) in case of documents stored on paper, store the document containing the personal data identified by the data subject separately from the other documents, in a sealed envelope, and hand it over to the data subject in such a way that no copy or duplicate remains in possession of the University.

In his/her request, the data subject shall indicate until what date he/she requests the restriction. If the data subject did not identify this date in his/her request, the University shall ask him/her via e-mail – or in case an e-mail address is not available, via postal mail – to specify until what time he/she requests the restriction.

(4) The data subject may request the restriction of the processing in case of exercising the right to object. In such a case, the University shall restrict the processing for the period of time during which the well-founded nature of the objection is examined. The University shall:

a) in case of electronically stored data, restrict access to such data;
b) in case of documents stored on paper, store the document containing the contested data separately from the other documents, in a sealed envelope.

If the request of the data subject is well-founded, the University shall delete the personal data.

Right to data portability

Section 27

(1) If the legal basis of the processing is the consent of the data subject or a contractual relationship, and the processing is automated, the data subject shall be entitled to

a) receive the personal data pertaining to the data subject and made available by him/her to the University in a structured, commonly used and machine-readable format, or

b) to have such data transmitted to another controller without hindrance from the University.

(2) Where technically feasible, the data subject shall have the right to have the personal data transmitted directly from between the University and the other controller identified by the data subject.

(3) In case of Subsection (1), point a), the University shall save the personal data to an external storage medium (such as a USB flash drive or disc). The external storage medium can also be provided by the data subject.

The right of objection

Section 28

(1) The data subject shall have the right to object at any time against the processing of his/her personal data with the application of a balancing test as the legal basis [Article 6 (1), point f) of the GDPR].

(2) In case of an objection, it shall be examined if, with respect to the processing indicated, the University has an opportunity to delete the personal data due to the facts and reasons referenced by the data subject, or to discontinue the processing with respect to the data subject.

(3) The University may continue to process the personal data if it is able to demonstrate that

a) there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject;

b) the processing is related to submitting, enforcing or defending a legal claim.

The identification of the data subject

Section 29

(1) If the University has reasonable doubts concerning the identity of the natural person making the request, it may require the provision of additional information

necessary to confirm the identity of the data subject. In the course of the above, the University may take the following steps:

a) calling the data subject by telephone to verify some of his/her further personal data available to the University, and in case of correct answers, his/her identity may be accepted as confirmed;
b) asking the data subject to submit his/her application in a private document of full conclusive force;
c) asking the data subject to present his/her personal identification document (nationality card, driving license, passport) at the premises of the University.

(2) If the data subject offers an alternative method for the confirmation of his/her identity and the University agrees, such alternative method may also be acceptable for the confirmation of his/her identity. The University itself may also offer an alternative method.

Deadline for compliance with the request
Section 30

(1) The University shall comply with the data subject's request within 1 month after receiving the same. The date when the request is received shall not count into the above time period.

(2) The above period may be extended by two further months where necessary, taking into account the complexity and the number of the requests. The University shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Compliance with the data subject's request
Section 31

(1) The University shall only comply with requests of the data subject submitted electronically or on paper *(Annex 5)*. Requests submitted by telephone may not be complied be. The University shall inform the data subject of this during the telephone call. In case the data subject submits his/her request at the premises of the University verbally, the request shall be drawn up in writing.

(2) The University shall comply with the request of the data subject in such form as requested by him/her.

(3) If the data subject submitted the request electronically, and also requests the copy of the data in electronic form, the University shall make this copy available in a commonly used, electronic format.

(4) If the data subject did not specify in his/her request in what format the answer is needed, the University shall contact the data subject and clarify in what form he/she wishes to receive the copy. Such making of contact shall be primarily by way of a telephone call or electronic mail; if these are not possible, the data subject shall be contacted by postal mail.

(5) The University shall comply with the data subject's right identified in the request. If the request of the data subject is not clear and it cannot be determined on the basis of the request which right the data subject wishes to exercise, the University shall contact the data subject to clarify this.

(6) If the data subject wishes to exercise more than one right in the request, each of these shall be complied with (e.g. in case of the simultaneous exercise of the right of access and the right to erasure, the University shall, on the one hand, inform the data subject about what personal rights are being processed, and on the other hand, delete the personal data, unless there is an exception, and shall inform the data subject of the above.

(7) The request of the data subject shall be performed free of charge.

Refusal of the data subject's request
Section 32

(1) The data subject's request may only be refused if a provision of EU or national law restricts or excludes the exercise of the rights of the data subject for the protection of the interests listed in Article 23 (1).

(2) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the University may refuse to act on the request.

(3) No fee may be charged for the refusal of the data subject's request.

(4) If the University does not act on the data subject's request, it shall inform the data subject, within 1 month:
   a) the reasons in terms of fact and law causing the measure not to be taken (on the basis of what provision of the GDPR or law could compliance with the request be refused);
   b) that the data subject may lodge a complaint with a supervisory authority and may exercise his/her right to legal remedy.

CHAPTER V

FUNDAMENTAL DATA SECURITY MEASURES

IT security measures
Section 33

(1) In the course of all processing, the University shall take such IT security measures, in case of IT systems including personal data, that:

a) prevent unauthorized persons from gaining access to logging into these systems;
b) regulate the setting of the appropriate access privileges, and assign user names and passwords to the individual privileges, and regulate the rules of password use (e.g. the minimum length of the password, the characters that may be used, terms of validity, number of incorrect passwords entered before the account is locked);
c) ensure that authorised persons may only gain access to personal data within the framework of their rights of access;
d) by way of logging, ensure that it may be determined and verified which user entered into and what software;
e) make it possible to determine and verify what personal data were entered, modified or transmitted by who and when;
f) ensure that the personal data cannot be read, copied, modified or removed without permission;
g) guarantee network security (e.g. by way of firewalls, intrusion detectors, as well as other active and passive systems providing for network security);
h) provide for the appropriate protection against viruses and other malware;
i) provide for the protection of the workstations (e.g. automatic locking, regular updates);
j) provide for the continuous availability of the systems;
k) in case of physical or technical incidents, ensure the capability that access to the personal data and the availability of the data can be restored in a timely manner, that a report is made of such incidents, and that these incidents have no effect on the integrity of the data;
l) where justified for the purpose of the given processing, guarantee the pseudonymisation and encryption of personal data;
m) where possible and justified for the purpose of the given processing, guarantee that the personal data (or the individual databases) are stored separately, through which measure, in case of a personal data breach, the likelihood of the personal data be associated with each other;
n) ensure that in case of using a processor, appropriate safeguards apply also to such processor's activities (e.g. the encryption of the personal transmitted to them, management and authentication of access privileges).

(2) The director of the IT Service Centre shall, by way of maintaining the records according to *Annex 6* of the internal privacy policy, document the fact that the IT systems of the University fully comply with the requirements listed in Subsection (1) above.

(3) The request for setting up an access privilege shall be submitted by the head of the organisational unit engaged in the processing to the head of the IT Service Centre.

(4) The employees may only use IT devices provided by the University for the storage of business secrets (including protected know-how), bank secrets and personal data managed by the University. The employees may not store such data on IT devices owned by themselves or by others.

(5) The employees may not use the e-mail address created by the University for their employees (hereinafter: university e-mail address), and may not store any personal data in the account belonging to the university e-mail address. Private use shall include, in particular, the sending or receiving of any e-mail message that is not related to the position of and the performance of work by the employee, or is not done in the interest of the University. E-mail messages of such content shall be deleted by the employees without delay.

(6) Employees engaged in the operation of the IT systems shall, to the extent necessary for the performance of their work, have access to personal data; however, they shall not use the data for other purposes, and shall not disclose the same to others.

Organisational security measures
Section 34

(1) In the course of all processing, the University shall take such organisational security measures, in case of IT systems including personal data, that:
   a) ensure that only authorised persons may enter certain premises;
   b) the data are stored on devices in rooms that are properly locked, dry, and equipped with fire protection and security equipment;
   c) filing cabinets in which documents containing personal data are stored shall be accessible only by specific persons;
   d) access to documents containing personal data shall be permitted to such persons only for whom it is indispensable to have access to these documents for the performance of their work;
   e) documents in continuous, active management shall be accessible to authorised persons only;
   f) employees may only leave the premises where documents containing personal data are stored or work is performed on such documents, either

during or at the end of the day, after locking away the documents or locking the office itself;

(2) All employees of the University shall maintain the confidentiality of business secrets (protected know-how), bank secrets and personal data managed by the University during the term of their legal relationship with the University. This obligation shall also survive the termination of the legal relationship.

CHAPTER VI

THE HANDLING AND REPORTING OF PERSONAL DATA BREACHES

The handling of personal data breaches
Section 35

(1) In case of the University, personal data breaches shall include, in particular:
   a) unauthorised access to IT systems or software storing or managing personal data;
   b) the unauthorised encryption of the personal data, as a result of which, even if only temporarily, the personal data become inaccessible or impossible to use;
   c) if an employee of the University gains unauthorised access to personal data, in an extent exceeding his/her level of authorisation, or performs data handling operations without (e.g. saving a database including personal data to an external data storage device) without authorisation;
   d) the intentional or negligent disclosure of personal data, without authorisation;
   e) making a document containing personal data accessible to others;
   f) the sending of an item of postal mail containing personal data to the wrong addressee;
   g) the sending of an e-mail containing personal data to the wrong addressee;
   h) the loss of data storage medium or IT device on which personal data are stored;
   i) damage to or destruction of an IT device on which personal data are store (including damage or destruction caused by fire or water), as a result of which the personal data become inaccessible – even if only temporarily – and cannot be used in the course of the processing activities of the University.

Finding out about a personal data breach
Section 36

(1) The University shall be deemed to have found out about the personal data breach when
   a) a circumstance referring to the occurrence of a personal data breach is discovered by an employee of the University;
   b) a message or letter sent to the University via e-mail, postal mail or other means of communication includes a reference to the occurrence of a personal data breach (even in case the message or letter is sent anonymously);
   c) a reference to the occurrence of a personal data breach appeared in the press on another website, of which the University learns or is notified of;
   d) a processor retained by the University gives notice of the fact via e-mail that a personal data breach occurred in connection with the personal data managed by the University.

(2) Employees of the University may also give notice of the occurrence of a personal data breach after logging in through the www.adatvedelem.unideb.hu page, under the menu item "Reporting personal data breach" or by way of an e-mail message sent to the the Data Protection Officer at adatvedelmi.tisztviselo@unideb.hu.

(2a) Employees of the University may also give notice of the occurrence of a personal data breach involving data concerning health after logging in through the www.adatvedelem.unideb.hu page, under the menu item "Reporting personal data breach" or by way of an e-mail message sent to the the Health Data Protection Officer at egeszsegugyi.tisztviselo@unideb.hu.

(3) Employees of the University shall notify their direct supervisor, the area Data Protection Officer, or the Data Protection Officer of the University, without delay, following the hierarchical chain. Certain organisational units may determine separate internal rules applicable to their own procedures in the stage preceding the notification of the Data Protection Officer.

(4) If an employee of the University believes that his/her direct supervisor may be affected in the given case, the supervisor of his/her supervisor shall be notified instead.

The suspension of the processing in case of a personal data breach
Section 37

(1) Following the notification concerning a personal data breach, the processing that is affected by the personal data breach shall be suspended without delay.

(2) The suspension may be ended, in particular, if:

a) on the basis of the available information, the personal data breach did not have serious consequences, and such consequences are not expected either;
b) after the suspension, the University took such measures that ensure that the personal data breach does not have serious consequences, and such consequences are not expected either;

(3) The decision on ending the suspension shall be made by the Chancellor, on the basis of the recommendation of the Data Protection Officer. The recommendation shall cover the following:
a) what kind of personal data breach occurred (the type and amount of the personal data, the number and categories of data subjects, what were or could have been the consequences on the data subjects);
b) why the ending of the suspension is recommended.

The reporting and investigation of the personal data breach
Section 38

(1) The University shall notify the fact of the personal data breach within 72 hours after becoming aware of the same, by way of the Data Protection Officer, using the website of NAIH, regardless of the amount of information available to the University in connection with the personal data breach. If the University fails to satisfy this notification obligation by the above time limit due to some obstacle, the obligation shall be satisfied without delay after the obstacle is removed, and a declaration exploring the reasons for the delay are also enclosed with the notification.

(2) The investigation of the personal data breach shall be commenced immediately after the suspension of the processing. In the course of the investigation, the following circumstances need to be clarified:
a) the type of the personal data breach (confidentiality, integrity or availability);
b) the measures used before the occurrence of the personal data breach;
c) the cause (likely cause) of the personal data breach;
d) the type and amount of personal data affected by the personal data breach (at least by way of estimation);
e) the number of data subjects (at least by way of estimation);
f) the categories of the data subjects, especially if there are vulnerable persons among (e.g. children, elderly, nationals of other countries) among those affected by the personal data breach;
g) how simple the identification of the data subject is on the basis of the group of data affected by the personal data breach;
h) the possible or occurred consequences of the personal data breach, and the seriousness of these on the data subjects;
i) whether it is necessary to inform the data subjects concerning the personal data breach, and if not, the reason for this;

j) what measure can be used to mitigate or eliminate the consequences of the personal data breach.

(3) The investigation of the personal data breach shall be carried out by the Information Security Emergency Team of the University of Debrecen (hereinafter: Emergency Team) (*Annex 7*).
The Data Protection Officer, the head of the IT Security Centre and the director of the IT Service Centre shall be the permanent members of the Emergency Team. In addition to the permanent members, additional members of the Emergency Team may be:
a) the head of the organisational unit affected by the personal data breach;
b) the area Data Protection Officer of the organisational unit affected by the personal data breach;
c) the person reporting the personal data breach;
d) if the personal data breach occurred in the course of the activity of a processor retained by the University, the representative of the processor.

(3a) If, as a result of the investigation, the Emergency Team finds that the personal data breach is of IT nature, the further investigation shall be carried out and the necessary measures shall be taken by the IT Security Centre and the IT Service Centre, and they shall inform the Data Protection Centre of the results thereof.

(4) If the independence or efficiency of the investigation of the personal data breach cannot be ensured within the organisation of the University, an external expert shall be retained for the investigation of the personal data breach.

(5) All new circumstances identified in the course of the investigation of the personal data breach shall be immediately notified by the Data Protection Officer to NAIH:

Dispensing with the reporting of the personal data breach
Section 39

(1) In case it is proven that a personal data breach occurred, however, it can also be determined at the time when the University becomes aware of the breach that it is not likely to impose any risk on the data subjects, it shall not be necessary to report the breach to NAIH.

(2) Such personal data breaches include in particular, when postal mail containing personal data and sent to a wrong address of a data subject is returned to the University unopened.

(3) The decision on dispensing with the reporting of the personal data breach shall be made by the Chancellor, on the basis of the recommendation of the Data Protection Officer. The recommendation shall cover the following:

a) what kind of personal data breach occurred (the type and amount of the personal data, the number and categories of data subjects, what were or could have been the consequences on the data subjects);
b) why a personal data breach constituting a risk for the data subjects did not occur;
c) how the occurrence of a similar personal data breach can be avoided in the future, provided that this question can be interpreted in connection with the given personal data breach;
d) why it is recommended that the University dispense with making a report to NAIH.

(4) If the Chancellor accepts the recommendation, the personal data breach shall be entered in the records of personal data breaches. The records of personal data breaches shall be maintained by the Data Protection Officer *(Annex 8)*.

Informing the data subjects
Section 40

(1) If the personal data breach is likely to result in a high risk for the data subjects, the University shall, without undue delay, notify the data subjects concerned of the personal data breach.

(2) The personal data breach shall be considered to have a high risk, in which case the data subjects need to be informed, if the personal data breach applies to one of the following categories of data:
a) sensitive data;
b) data pertaining to the financial position of the data subject (e.g. debt);
c) data having an effect on the social standing of the data subject (e.g. weak academic results);
d) user name, password;
e) data suitable for identity theft.

(3) The information provided for the data subject shall include:
a) the nature of the personal data breach;
b) the name and contact details of the other contact point where more information can be obtained,
c) information on the possible or occurred consequences of the personal data breach, and the seriousness of these on the data subjects,
d) the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects arising from the personal data breach;

(4) The information in advance shall be sent to the e-mail addresses of the data subjects. If the e-mail addresses of the data subjects are not available, the information shall be sent to their postal addresses. If there are data subjects who

could not be informed about the personal data breach, or the sending of information to all data subjects concerned would require disproportionate effort, a notice may also be published on the website.

(5) The Data Protection officer shall make a recommendation concerning the text of the notification according to subsection (3) and the format according to subsection (4), and the decision shall be made by the Chancellor.

(6) The provision of information in advance may be dispensed with if:
   a) the University has implemented appropriate data protection measures, and those measures were applied to the personal data affected by the personal data breach, including measures in particular that render the personal data unintelligible to any person who is not authorised to access it (for example, using methods of encryption);
   b) the University took such further measures after the personal data breach that ensure that the personal data breach would likely not involve high risks for the data subjects.

(7) The decision on dispensing with the provision of information in advance for the data subjects shall be made by the Chancellor, on the basis of the recommendation of the Data Protection Officer. The recommendation shall cover the following:
   a) what kind of personal data breach occurred (the type and amount of the personal data, the number and categories of data subjects, what were or could have been the consequences on the data subjects);
   b) why it would be necessary to inform the data subjects;
   c) why it is recommended that the University should not inform the data subjects concerning the personal data breach.

Written record of the investigation and the record of personal data breaches
Section 41

(1) The results of the investigations of personal data breaches shall be drawn up in writing, in which a recommendation shall also be made for remedying the personal data breach and eliminating its causes. The decision on selecting and introducing the necessary measures shall be made by the Chancellor.

(2) Records in accordance with the internal privacy policy shall be kept of all personal data breaches occurring at the University, regardless of whether or not a report had to be sent to the NAIH.

(3) The records of the breaches shall be kept separately for each personal data breach, in such a way that enables NAIH to check compliance with the applicable provisions of law. The records of personal data breaches shall be maintained by the Data Protection Officer.

CHAPTER VII

THE DATA PROTECTION OFFICER AND THE DATA SECURITY CENTRE

Provisions applicable to the Data Protection Officer
Section 42

(1) In the interest of ensuring the performance of the legal requirements pertaining to the processing of personal data and promoting the enforcement of the rights of the data subjects, the University shall employ a Data Protection Officer.

(2) The tasks of the Data Protection Officer:

a) providing information and professional advice for the University and the employees in connection with their obligations under the applicable law;
b) helping data subjects in the exercise of their rights, and in particular, investigating their complaints, and initiating the taking of measures necessary for remedying complaints;
c) monitoring compliance with the applicable law and with the policies of the University in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
d) cooperating with NAIH, acting as a point of contact for NAIH, and if necessary, engaging in consultation with them in any question as necessary;
e) performing the tasks assigned to him/her on the basis of the present internal privacy policy, participating in the processes of drafting and amending the internal privacy policy;
f) performing all tasks assigned to him or her by the Chancellor;
g) maintaining the data map of the University;
h) maintaining the following records:

- the records of the Data Protection Officer's tasks (*Annex 9*)
- the records of personal data breaches;
- records of the reports submitted by the Data Protection Officer;
- maintaining records of teaching activities;

i) in the interest of reinforcing awareness about the issues of data protection, giving lectures at the University. *(Annex 10).*

(3) The Data Protection Office shall have the right to check compliance with the provisions of the GDPR and other provisions of law, as well as with internal policies of the controller related to the protection of personal data. The Data Protection Office may inspect the data processing. The Data Protection Office may request information, either verbally or in writing, from heads and

employees of the units engaged in data processing. In case of a breach of the law, the Data Protection Officer shall call upon the controller to eliminate such breach, and shall report the breach to the Chancellor. The Data Protection Officer shall report the findings made in the course of the investigations to the Chancellor of the University, without delay after the closing of the investigations.

(4) The University shall:

a) ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;
b) support the Data Protection Officer in performing his or her tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge;
c) ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks;
d) ensure that in case the Data Protection Officer also performs other tasks, there should be no conflict of interest from these tasks.

(5) The University shall ensure that the Data Protection Officer should report directly to the Chancellor.

(6) The Chancellor may not dismiss or penalise the Data Protection Officer for reasons related to performing his or her tasks.

(7) The University shall notify the address and the contact information of the Data Protection Officer to NAIH for inclusion in the latter's records.

(8) The contact information of the Data Protection Officer is the following: adatvedelmi.tisztviselo@unideb.hu. The contact information has been published on the website of the University at: https://unideb.hu/hu/adatvedelmi-tiszviselo.

(8a) The Health Data Protection Officer shall be competent to act in issues related to the processing and protection of personal data concerning health, who shall cooperate with the Data Protection Officer in the course of discharging his/her duties. Further the Health Data Protection Officer shall have the obligation to report breaches involving personal data concerning health to the Data Protection Officer of the University.

(8b) The contact information for the Health Data Protection Officer is the following: egeszsegugyi.tisztviselo@unideb.hu. The contact information has been published on the website of the University at: https://unideb.hu/hu/adatvedelmi-tiszviselo.

(9) The Data Protection Officer shall keep in confidence, during his/her appointment to this office such and also thereafter, all personal, classified, and other data considered as protected by law and data considered as secrets related to the exercise of a profession, as well as all such data, facts or circumstances that the controller or processor employing the Data protection officer is not required by law to make accessible to the public.

(10) The information materials related to the tasks of the Data Protection Officer shall be available, after logging in, on the website of the Chancellor's Office, under the "Data Protection" menu item.

Cooperation with the supervisory authority

Section 43

(1) Any inquiries and decisions received from the supervisory authority, including in particular NAIH, shall be forwarded to the Data Protection Officer without delay.

(2) The Data Protection Officer shall, not more than four days before the deadline indicated in the inquiry or decision, submit a proposal to the Chancellor. A reply to the inquiry or decision of NAIH may be sent with the signature of the Chancellor.

Data Protection Centre
Section 44

(1) The Data Protection Officer shall be assisted in the performance of his/her tasks by a Data Protection Centre, operating with his/her professional supervision.

(2) The University shall ensure that the employees of the Data Protection Centre be involved, in the proper manner and time, in all issues related to the protection of personal data, support the employees of the Data Protection Centre in the performance of their tasks by way of providing the resources necessary for the performance of such tasks, access to the personal data and the data processing operations, and for the maintenance of expert-level knowledge, ensure that the employees of the Data Protection Centre can accept no instructions in connection with the performance of their tasks from anyone, with the exception of the Data Protection Officer, and ensure that in case the employees of the Data Protection Centre also perform other tasks, there should be no conflict of interest from these tasks. The Chancellor may not dismiss the employees of the Data Protection Centre, or impose sanctions against them, in connection with the performance of their tasks related to data protection (including in particular for the formulation of their professional opinions).

Area Data Protection Officer
Section 45

(1) Each organisational unit of the University shall appoint an area Data Protection Officer (hereinafter collectively: the area Data Protection Officers) from among the employees of the University, whose names and contact information shall be notified by the head of the organisational unit to the Data Protection Centre of the University. The organisational units of the University of Debrecen may, in case of significantly complex tasks, as a necessity, appoint several area Data Protection Officers for the performance of the related tasks in the partial areas.

(2) The tasks of the area Data Protection Officer shall be in particular:
   a) checking the data processing and processing activities in the organisational unit in his/her area, and in the course of the above, having access to the files and documentation related to data protection, and submitting his/her report to the Data Protection Officer and to his/her supervisor;
   b) reporting any personal data breach that occurred or was detected in the organisational unit belonging to his/her area to the Data Protection Officer of the University and to his/her direct supervisor;
   c) indicating problems related to the processing and data protection to the Data Protection Officer of the University;

d) participating in regulating access to electronically processed data, as well as to the preparation and amendment of the University's data protection and data security policies;
e) preparing, with respect to the given organisational unit, the requests of the data subjects for the inspection, deletion of data and for restriction of controlling, and submitting the same to the head of the organisational unit; maintaining the records related to the above;
f) with the participation of the Data Protection Centre, participating in the strengthening of data protection awareness, as well in the provision of training;
g) cooperating with the staff members of the Data Protection Centre.

(3) The area Data Protection Officer shall be bound by a confidentiality obligation, which shall survive the termination of his/her employment by the University.

CHAPTER VIII

FURTHER OBLIGATIONS RELATED TO DATA PROCESSING

The use of processors
Section 46

(1) The University may only use such processors who or which provide appropriate safeguards for satisfying the requirements of the GDPR.

(2) The University may follow three procedures in connection with the use of a new processor:
a) if the processor presents an internal policy, submits a declaration, or publishes an undertaking of obligation on its website on the basis of which it can be clearly established that the activities of the processor are in compliance with the GDPR, then the University may accept this in itself, and shall not have to use points b) or c);
b) if the requirements in point a) are not satisfied, and the activities of the processor do not constitute a high risk from the point of view of the University's processing, the declaration included in *Annex 11* to the internal privacy policy shall be sent to the processor;
c) if the processor is engaged in activities constituting a high risk from the point of view of the University's processing, the conclusion of the data processing agreement in accordance with *Annex 12* shall be necessary.

(3) In case of using a new processor, the head of the organisational unit concerned shall decide which of the procedures in Subsection (2) shall be used by the

University. When necessary, the opinion of the Data Protection Officer shall be obtained.

Data protection impact assessment
Section 47

(1) The University shall carry out an impact assessment if, based on its nature, scope, context and purposes, the processing is likely to result in a high risk to the rights and freedoms of natural persons.

(2) A data protection impact assessment shall be carried out, in particular, if
   a) the University is engaged in processing that is based on a systematic and extensive evaluation of the data subjects, and on which decisions are based that produce legal effects concerning the data subjects;
   b) the University engages in a systematic monitoring of a publicly accessible area;
   c) the processing activity of the University is included in the register published by NAIH in connection with the performance of data protection impact assessments.

(3) The data protection impact assessment shall encompass at least the following:
   a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the University;
   b) the provisions of the applicable law, as well as, where possible, the established practice or the NAIH or the courts;
   c) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   d) an assessment of the risks to the rights of data subjects, as well as the measures aimed at managing those risks.

(4) The University may also perform the impact assessment with the use of the data protection impact assessment software published by NAIH on its website.

(5) If, after the mitigation of the risks identified by the University in accordance with Subsection (3), point d), the processing is still considered to have a high risk, NAIH shall be contacted with the request for prior consultation. Based on the recommendation of the Data Protection Officer, the Chancellor shall decide whether it is necessary to contact NAIH in the interest of prior consultation.

(6) The data protection impact assessment shall be carried out by the organisational unit concerned; if requested, the Data Protection Officer shall provide professional advice with respect to the data protection impact assessment, and shall monitor the performance of the impact assessment. The results of the

impact assessment shall be approved by the Chancellor. If the independence or efficiency of the impact study cannot be ensured within the organisation of the University, an external expert shall be retained for the performance of the data protection impact study.

Joint processing

Section 48

(1) If the controller performs the processing jointly with another controller, then the two controllers shall conclude an agreement in accordance with *Annex 13* of the internal privacy policy.

(2) The jointly performed processing shall not be commenced, or processing already commenced shall be suspended, until such time when all controllers participating in the jointly performed processing signed the agreement.

(3) In case the suspension of the jointly performed processing would disproportionately impair the activity of the University, and there is no high risk inherent with the jointly performed processing from the perspective of the University's activities, then the suspension may be ended.

(4) The decision on ending the suspension shall be made by the Chancellor, on the basis of the recommendation of the Data Protection Officer. The recommendation shall include:
   a) the description of the joint data processing
   b) why the ending of the suspension is recommended.

CHAPTER IX

RESPONSIBILITY FOR COMPLIANCE WITH THE RULES OF DATA PROCESSING, CONTROLS

Section 49

(1) The University's Data Protection Officer/Area Data Protection Officers shall not substitute for the heads and staff members of the individual organisational units in terms of their personal responsibilities related to processing and compliance with the data protection requirements, but shall support and coordinate the same.

(2) Compliance with the requirements related to data protection, including in particular with the provisions of the present policy, shall be checked by the heads of the organisational units engaged in processing activities on a continuous basis.

(3) When detecting the violation of a provision related to data protection, the head of the organisational unit shall take immediate measures for the elimination of the violation, with the participation of the area Data Protection Officer and the Data Protection Officer. If such measures are not successful, they shall notify the Rector and the Chancellor by way of the University's Data Protection Officer, who shall, in case of particularly serious cases of violations, initiate that the responsible persons be identified, and in justified cases a procedure to recover damages be started, and shall take the necessary measures to restore lawfulness.

(4) With prior notification given to the head of the relevant organisational unit, the Rector and the Chancellor of the University shall have an unrestricted right of inspection, while the Vice Rectors and the heads of the organisational units (also including presidents of committees and other bodies) shall have a right of inspection within their respective areas of competence, into the processing activity at the organisational units. The leaders may assign their rights of inspection to other persons. The personal data accessed in the course of such inspection shall be subject to a confidentiality obligation.

(5) The persons engaged in the processing shall be required to keep the personal data they have access to as institutional secrets, and shall make all efforts to ensure their proper protection. Only such persons may be employed in these positions who have made a declaration of confidentiality.

(6) If such a person, on the basis of his/her position or office, gains access or comes into the possession of personal or sensitive data, or personal data relating to criminal convictions and offences, they shall proceed in compliance with the provisions of the Information Act, and thus, they may only use the personal data for the previously determined purpose and shall protect such data from unauthorised access.

(7) The private-purpose use of the personal data processed by the University, or transmitted by another controller for the performance of the tasks of the University, shall be prohibited.

(8) If the controller finds out that the personal data processed by it is incorrect, incomplete or obsolete, it shall correct the data, or initiate with the staff member recording the data the correction of the same.

CHAPTER X
DATA TRANSMISSION

Data transmission
Section 50

(1) In case of the transmission of personal data by postal mail, it shall be ensured that it is sent in a sealed envelope. In case of the electronic transmission of personal data, appropriate measures of security and protection shall be taken.

(2) The personal data processed by one organisational unit of the University may only be transmitted to another competent organisational unit of the University for the purpose of performing the tasks, to the extent necessary for such tasks, and in case the appropriate legal basis is in place. When determining the lawfulness of data transmission, it shall be taken into account whether the organisation requesting the data is entitled to process the data requested.

(3) Any requests for the transmission of data received from a body outside the University or from a private individual may only be performed if permitted by law or a specific provisions of the GDPR.

(4) If the organisational unit processing the data receives a request for personal data, and is unable to determine the lawfulness of the request, it shall notify the request to the Data Protection Officer of the University and obtain his/her recommendation.

Obligations related to data transmissions to third countries
Section 51

(1) The University may only transmit personal data to processors located in third countries, or employ a processor located in third countries in case the conditions prescribed in the applicable law and in the internal privacy policy are satisfied.

(2) If a legislative act of the European Union or a national law has determined that a third country, a territory or a specified sector within a third country, or an international organisation in questions ensures an adequate level of data protection, then there is no obstacle to the transmission of the personal data in this respect.

(3) If the Commission of the European Union has not adopted a resolution in connection with the data transmission, the University may choose from the following legal means:
   a) adopting binding corporate rules, or participation in the application of such rules;
   b) standard data protection clauses adopted by the Commission of the European Union;
   c) standard data protection clauses adopted by NAIH and approved by the Commission of the European Union;
   d) contractual clauses between the University and another controller or processor approved by NAIH.

(4) Data transmission to a third country shall also be lawful in case:
   a) the controller or processor located in a third country accepts the codes of conduct pursuant to Article 41 of the GDPR as binding upon itself, and makes a binding and enforceable commitment in connection with the above;
   b) the controller or processor located in a third country accepts the certification mechanism pursuant to Article 43 of the GDPR as binding upon itself, and makes a binding and enforceable commitment in connection with the above;

(5) If subsections (2) to (4) cannot be applied, in exceptional cases, the transfer of personal data to a third country may also be permitted if:
   a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
   b) the transfer is necessary for the performance of a contract between the data subject and the University or the implementation of pre-contractual measures taken at the data subject's request;
   c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the University and another natural or legal person;
   d) the transfer is necessary for important reasons of public interest;
   e) the transfer is necessary for the establishment, exercise or defence of legal claims;
   f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
   g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Records of data transmissions
Section 52

(1) Records of data transmissions outside the University shall be kept within the organisational unit making the transmission of the data; such records shall include the date, the legal basis and the recipient of such transmission, the definition of the scope of the data transmitted, as well as other information as

required by law. The records shall be sent to the Data Protection Officer of the University *(Annex 14).*

CHAPTER XI

Electronic monitoring system
Section 53

(1) An electronic **monitoring** system operates at the University.

(2) The University shall ensure that visitors to the buildings of the University receive prior notice and information, in the detail prescribed by law, about all important requirements of the processing related to the electronic **monitoring** system. The privacy notice of the CCTV system is available on the website of the Chancellor's Office.

CHAPTER XII

MISCELLANEOUS AND CLOSING PROVISIONS

Section 54

(1) The head of the organisational units, the University Student Government and its constituent student governments, as well as the University Doctoral Student Union and the presidents of the doctoral students' representative bodies operating within the framework of the above, shall comply with and enforce compliance with the provisions of the present policy.

(2) The heads of the institutes of public education maintained by the University shall ensure that the present policy is duly applied to persons working for them as employees or on the basis of a retainer agreement, as well as to their students and trainee teachers.

(3) The present Policy was approved by the Senate of the University of Debrecen at its meeting held on 21 September 2021, by way of Resolution no. 16/2021 (XI. 23.). The Policy shall enter into effect on the day following its approval.

(4) Upon the present Policy entering into effect, it shall supersede the Internal Data Protection Policy of the University of Debrecen, adopted by the Senate at its meeting held on 24 January 2019 by way of resolution no. 26/2019 (I. 24.).

Debrecen, 23 September 2021

Prof. Dr. Zoltán Szilvássy
rector

Prof. Dr. Zoltán Bács
chancellor

ANNEXES

Annex 1

Questionnaire for the application of the balancing of legitimate interests as a legal basis

1. Compliance with the basic principles in the course of the processing

1.1. What activity of the ..... (faculty, organisational unit) of the University of Debrecen makes the processing of personal data necessary?

1.2. Can this activity be performed with the use of a different method, without the processing of personal data?

1.3. The verification of the principle of data minimisation:

Processed personal data	The reason for the processing of the specific personal data
Example: name	*Example: the reliable identification of the data subjects in the contract concluded with them*

1.4. What is the duration of the processing? What is the reason why processing is necessary for this duration?

1.5. What group of data subjects does the processing apply to?

1.6. Is there a vulnerable group of data subjects that would require additional measures of protection? *(e.g. elderly, children)*

2. The necessity test

2.1. Why is the processing important for the controller? *(Even if the interest related to the processing is obvious to all and also lawful for our purposes, it needs to be properly explained to the data subjects. The fact that the processing constitutes the basis of the Controller's activities does not, in itself, make the processing lawful.)*

2.2. If there is a third party involved in the processing, why is the processing important for us?

3. Proportionality

3.1. Can data subjects expect processing without their consent, on the basis of the balancing of legitimate interests as the legal basis?

3.2. Does the processing have added value with respect to the product or service used by the data subjects?

3.3. Can the processing have an adverse effect on the rights of the data subjects?

3.4. Can the processing cause unreasonable damage or other disadvantage for the data subjects?

3.5. Will it have an adverse effect on the Controller if it is not able to engage in the processing?

3.6. Will it have an adverse effect on the the third party if it is not able to engage in the processing?
Answer:

3.7. Is the processing also in the interest of the data subjects?

3.8. Are the legitimate interests of the data subjects and the Controller (or the third party) identical?

3.9. Does the processing constitute a (local or wider) social interest?

3.10. What is the relationship between the data subject and the controller? *(E.g. student, former student, employee, person performing work under a retainer or service contract, business partner, prospective student who is not yet affiliated with the University.)*

3.11. What is period does the relationship between the data subject and the controller encompass? *(E.g. there is a continuous relationship between the controller and the data subject, or they are in a relationship periodically, or there was only a single*

occasion when there was a relationship between them, or there was no prior relationship between them before the processing.)

3.12. What personal data does the processing apply to? Does the processing involve sensitive data?

3.13. Does the processing prevent or restrict the data subjects' possibility to exercise their rights in accordance with Articles 15 to 22 of the GDPR?

3.14. Does the Controller obtain the personal data directly from the data subjects or indirectly, from a different source?

3.15. Can the data subject expect that the Controller would process their data for the purposes of the proposed data processing?

3.16. Can the data subjects consider the processing intrusive or disproportionate relative to the nature of the processing?

3.17. Was a clear and transparent notice on data processing prepared in appropriate detail?

3.18. Can data subjects exercise control in connection with the processing of their personal data, including in particular the possibility to ask for their personal data to be erased? If the data subjects have no control, what is the reason for this?

3.19. Can the circumstances of the processing (e.g. the scope of the data subjects and of the personal data covered, the duration of the processing) be narrowed down or reduced?

4. The rights affected by the balancing of interests as the legal basis

4.1. How does the processing restrict the data subjects' right of disposal over their personal data? *(E.g. the data may be published without their consent, other persons may have access to the data)*

4.2. Can the processing affect other freedoms or interests of the data subjects? *(E.g. freedom of expression, respect for private and family life, home and communications, the right to an effective remedy and to fair proceedings.)*

4.3. What expectations can (do) the data subjects have against the Controller in terms of safeguards during the processing?

5. Safeguarding measures during the processing

It must be presented what safeguarding measures the Controller uses in order to reduce the the negative effects of the processing on the data subjects. Such measures may be, for example (based on the nature of the processing, choose from the following, or insert additional measures):

- *reducing the scope of the personal data processed to the necessary minimum;*
- *reducing the duration of the data processing to the necessary minimum;*
- *allowing the data subjects to opt out of the processing at any time;*
- *the anonymisation of the data;*
- *the setting up on an interface on which the data subjects can monitor which of their personal data are being processed;*
- *providing additional information for the data subjects (e.g., the privacy notice and the balancing test is also sent via e-mail);*
- *only a certain, defined group of persons may have access to the personal data, and access is logged;*
- *multi-factor authentication when accessing the databases containing the personal data of the data subjects;*
- *the encryption or anonymisation of the database;*
- *in case of the monitoring of an employee, adhering to the principle of graduate measures (monitoring of the the employee should only take place if no other methods may be used for detecting violations) and ensuring the presence of the employee during the monitoring;*

Annex 2

Balancing test of legitimate interest

with respect to [designation of data processing]

1. The balancing of legitimate interests and its legal basis

Pursuant to point f) of Article 6 (1) f) of the GDPR, the processing of personal data may be regarded as lawful if "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data*."

In case this legal basis is used, the consent of the data subject is not required for the processing; instead, it is necessary that the University of Debrecen should be able to demonstrate for the data subjects:

- that it has a real and actual legitimate interest in the processing of the data;
- what rights the processing of the data affects, and what expectations the data subject may have in connection with the processing of the data;
- that it has introduced safeguards to guarantee that the data processing conducted on the basis of its legitimate interest only cause a proportionate restriction of the rights and the privacy of the data subjects.

The satisfaction of the above conditions is summarised by the University in a balancing test, in which it is shown what legitimate interest it has in the course of the [name of processing activity], and what safeguards were introduced to guarantee the protection of your rights.

2. Legitimate interests

In connection with the data processing, you have the following legitimate interest(s):

- [why it is advantageous for the controller]
- [why it is advantageous for the data subject]
- [it also belongs here when the processing is necessary for the performance of an obligation under a contract with another entity]

3. The expectations of the data subjects and the safeguards used

On the basis of our assessment, the processing performed by us does not affect your right to the protection of personal data.

In addition, in the course of our assessment, we have come to the conclusion that the following must be guaranteed in the course of our data processing:

- the scope of the processing should be limited to the indispensable data;
- only such persons should have access to the personal data in the case of whom this is actually justified in the interest of the performance of their tasks or work;
- due information should be provided on the processing of the data;
- in case of your protest, we should stop the processing (this could only be applicable in case of a few types of processing, such as processing for marketing purposes).

In order to guarantee that the processing of data only result in a restriction of the rights of data subjects to the extent necessary, we introduce the following safeguards:

- The duration of the processing shall be for .... days/years. This is justified because...
- The following data are necessary in case of this processing: (list the processed data). From among the above, the processing of the name, as well as the place and date of birth, is necessary because... The processing of the ... and ... data are important because...
- On the basis of our system of access rights, personal data are only accessible to employees working in the positions of ... and ... The personal data are not received by ....
- The present balancing test serves the purpose, among others, to ensure that you have sufficient information on the data processing.
- You can find a description of your rights and remedies available to you in the data protection policy (privacy policy), which is accessible (or downloadable) via the following link: .

Place and date, signature

Annex 3

Privacy Notice

The name and contact information of the Controller

[name of controller]

Registered address: ...
Postal address: ...
E-mail address: ...
Phone number: ...

2. Provisions of law governing the processing

The processing performed by the [name of controller] is governed by the following provisions of law:

- Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: GDPR);

- Act ... of ... on ..... (hereinafter: ...).

3. The processing activities performed by the Controller

3.1. Data processing related to .....

3.1.1. The purpose of the processing: ...

3.1.2. The scope of the processed data: In the course of the above, we process the following personal data:

- ...
- ...

3.1.3. The legal basis of the processing: ... (e.g. consent) [the exact designation of the legal basis according to the GDPR: Article 6 (1), point c) of the GDPR].

3.1.4. The duration of the processing: ...

3.1.5. The scope of those having access to the data: ...

3.2. Processing related to ...

3.2.1. The purpose of the processing: .....

3.2.2. The scope of the processed data: ...:

- ...

3.2.3. The legal basis of the processing: ...

3.2.4. The duration of the processing: ...

4. Your rights and the rules applicable to the exercise of such rights

4.1. Right to information

In accordance with Article 15 (1) of the GDPR, you may request information concerning the personal data processed by the [name of controller]. In such a case, using your contact information (e-mail address, postal address), the [name of controller] shall forward to you the following information:

- what personal data related to you we process;
- what are the purposes of the processing;
- to whom we transmit the personal data;
- the duration of the processing and the criteria for the determination of such duration;
- your rights related to the processing;
- your right to file complaints addressed to the National Authority for Data Protection and Freedom of Information.

4.2. The right to receive a copy of the data

In accordance with Article 15 (3)-(4) of the GDPR, you may request a copy of your data processed by [name of controller]. In such a case, using your contact information (e-

mail address, postal address), the [name of controller] shall forward to you the personal data that we process in connection with you.

4.3. Right of rectification

Pursuant to Article 16 of the GDPR, at your request, we modify or rectify your personal data.

4.4. Right to erasure

In the case of processing in accordance with Section 3.4 above, pursuant to Article 17 (1) of the GDPR, you may request the erasure of your disclosed personal data.

4.5. The right to restrict the processing

You may request the restriction of the data processing in the following cases:

- you contest the accuracy of the personal data, in which case we restrict the processing until the [name of controller] verifies the accuracy of the personal data;
- the data processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- the [name of controller] no longer needs the personal data, but you require them for the establishment, exercise or defence of legal claims; or
- you exercises the right of objection, in which case we restrict the processing of his or her data for the duration of verifying the lawfulness of your request.

In your request for the restriction of processing, you are required to indicate the reason for requesting the restriction.

The [name of controller] shall satisfy your request for the restriction of data processing by way of storing the personal data concerned separately from all other personal data. For example, in case of electronic data files, the personal data concerned shall be saved on an external storage medium, and in case of paper-based files, they shall be stored in a separate file.

4.6. Objection

You may object to the processing of your data carried out based on the balancing of legitimate interests for reasons related to your own situation. In such a case the [name of controller] shall examine the processing of data performed with respect to you on the basis of the balancing of legitimate interests, and if your request is found to be well-

grounded, we shall erase your personal data. In all cases, we shall inform you on the outcome of the above procedure of examination.

4.7. The joint rules of the exercise of rights

The [name of controller] shall perform your request within not more than one month, which time limit may be extended by at least two additional months.

In case of the refusal of the request, the [name of controller] shall inform you, within one month of the receipt of your request, of the reasons for such refusal, as well as your right to file a complaint to the Authority and your right to legal remedy.

The [name of controller] reserves the right in case of having any doubts concerning the identity of the person submitting the request to ask for further information as necessary for confirming the identity of the data subject concerned. Such cases include, in particular, where data subjects exercise their right to obtain a copy of their personal data, in which case it is justified for the [name of controller] to verify that the request is indeed from the data subject concerned.

5. Your opportunities for legal remedy

If, in your opinion, the processing performed by the [name of controller] is not in compliance with the relevant provisions of law, then you may file a complaint with the National Authority for Data Protection and Freedom of Information (postal address: 1363 Budapest, P.O. Box 9, e-mail address: ugyfelszolgalat@naih.hu) to initiate a procedure or may submit a claim to the courts.

Annex 4: Data processing records

Data processing records

Item no.	The name and contact information of the Controller	The designation of the processing	The purpose of the processing	Legal basis for processing	The starting date of the processing	The place of the processing	Categories of processing	The categories of data subjects (employees, students, teachers, pupils, attendees)	The recipients of the data transmitted, processed	data transmission into third countries or international organisations	Duration of processing (deadline for deletion, period of retention)	Form of data processed (e.g. paper, electronic, paper and electronic)	Technical and organizational measures for data security, type of storage (e.g. system with access rights, closed cabinet)

Annex 5

Request by data subject (recommended to be used)

Name of data subject: .....

Type and number of identification document: .....

Contact information of data subject: .....

Type of data processing request: Please underline as appropriate.

Request for information on data processed (Articles 13 and 14 of GDPR)
Access to personal data (Article 15 of GDPR)
Change of personal data (Article 16 of GDPR)
Deletion of personal data (Article 17 of GDPR)
Restriction of processing of personal data (Article 18 of GDPR)
Objection to the processing of personal data (Article 21 of GDPR)

The undersigned, I have the following request to the University of Debrecen as data controller:
.....
...
.....
...
.....
...
.....
...
.....
...
.....
...
.....
...

Place and date, signature

Annex 6

IT security measures

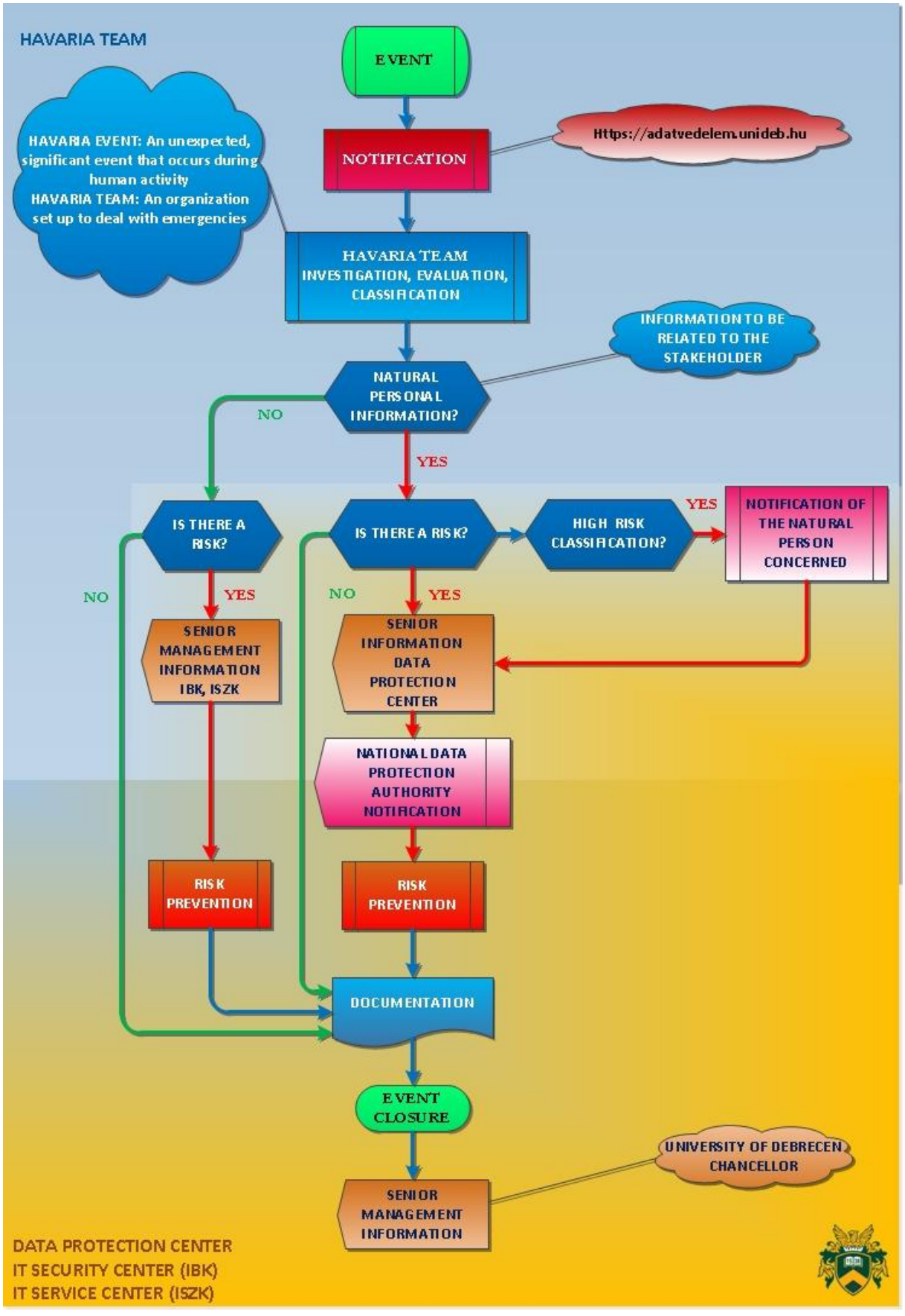
IT security measure	Solution used
Preventing unauthorized persons from gaining access to logging into these systems	
Setting up the appropriate rights of access, as well as the assignment of user names and passwords to each of the access rights	
Introducing requirements with respect to the use of passwords (e.g. the minimum length of the password, the characters that may be used, terms of validity, number of incorrect passwords entered before the account is locked)	
Ensuring that authorised persons may only gain access to personal data within the framework of their rights of access	
Ensuring, by way of logging, that it may be determined and verified which user entered into and what software	
Making it possible to determine and verify what personal data were entered, modified or transmitted by who and when	
Ensuring that the personal data cannot be read, copied, modified or removed without permission	
Ensuring the continuous availability of the IT systems	
Protective measures related to network safety	
Measures related to the protection against viruses and other malware	

Measures ensuring the protection of the workstations (automatic locking, regular updates)	
Measures ensuring the continuous availability of the IT systems.	
In case of physical or technical incidents, ensure the capability that access to the personal data and the availability of the data can be restored in a timely manner, that a report is made of such incidents, and that these incidents have no effect on the integrity of the data;	
The encryption or pseudonymisation of personal data (if justified in case of the given processing)	
Ensuring that the personal data (or the individual databases) are stored separately (if justified and possible in case of the given processing)	
Ensuring that in case of using a processor, appropriate safeguards apply to their activities (e.g. the encryption of the personal transmitted to them, management and authentication of access privileges).	

Place, date

Signature

Annex 7


HAVARIA TEAM
EVENT
HAVARIA EVENT: An unexpected, significant event that occurs during human activity
HAVARIA TEAM: An organization set up to deal with emergencies
NOTIFICATION
Https://adatvedelem.unideb.hu
HAVARIA TEAM INVESTIGATION, EVALUATION, CLASSIFICATION
INFORMATION TO BE RELATED TO THE STAKEHOLDER
NATURAL PERSONAL INFORMATION?
NO
YES
IS THERE A RISK?
IS THERE A RISK?
HIGH RISK CLASSIFICATION?
YES
NOTIFICATION OF THE NATURAL PERSON CONCERNED
NO
YES
NO
YES
SENIOR MANAGEMENT INFORMATION IBK, ISZK
SENIOR INFORMATION DATA PROTECTION CENTER
NATIONAL DATA PROTECTION AUTHORITY NOTIFICATION
RISK PREVENTION
RISK PREVENTION
DOCUMENTATION
EVENT CLOSURE
UNIVERSITY OF DEBRECEN CHANCELLOR
SENIOR MANAGEMENT INFORMATION
DATA PROTECTION CENTER
IT SECURITY CENTER (IBK)
IT SERVICE CENTER (ISZK)

Annex 8

Records of personal data breaches

Title: [the date and time of the personal data breach, the nature of the personal data breach]

1. The measures used before the occurrence of the personal data breach:

2. The nature of the personal data breach:

3. The cause of the personal data breach:

4. The type and amount of personal data affected by the personal data breach (at least by way of estimation):

5. The number of data subjects affected:

6. The categories of the data subjects:

7. The possible or occurred consequences of the personal data breach, and the seriousness of these on the data subjects:

8. If the Controller did not report the personal data breach, the reason for this:

9. If it was not necessary to inform the data subjects, the reason for this:

10. If it would have been necessary, but the Controller did not inform the data subjects, the reason for this:

11. The measures taken for remedying the personal data breach and for the elimination of its causes:

Annex 9

The record of the tasks performed by the (area) Data Protection Officer

Registration number/serial number	Date of measure	Name of measure	Description of measure	Result of measure

Annex 10

Attendance sheet for data protection training

Record of attendance

of the persons participating at the training/presentation at the University of Debrecen (venue of training, name of organisational unit, starting date and time) on the topic of (description of the topic of the training/presentation).

Serial no.	**Name of attendee** (Please print)	**Signature of attendee**	**Name of organisational unit**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

Annex 11

[Name of processor]

[Address of processor]

SUBJECT: Declaration of compliance with the GDPR

Dear [name of contact person],

As you are probably aware, in the framework of the services provided by the University of Debrecen (registered seat: 4032 Debrecen, Egyetem tér 1; hereinafter: Controller), you have access to personal data processed by the Controller, and thus you are considered as the processor of the Controller.

Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR) imposes many new obligations on the data controllers and processors.

Article 28 (1) of the GDPR expressly prescribes for controllers to only use such processors that can satisfy the requirements of the GDPR.

"Where processing is to be carried out on behalf of a controller, ***the controller shall use only processors*** *providing sufficient safeguards to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*

With a view to the above, we ask you that, in the interest of compliance with Article 28 (1) of the GDPR you complete and sign the declaration enclosed with our letter, and return it to us by postal mail.

Thank you for your cooperation! Please do not hesitate to contact us with any questions you may have.

[Place, date]

Sincerely,
[Signature]

The Processor's declaration of compliance with the GDPR

The undersigned as the representative of the Processor's name (registered seat, company registration number, tax number) (hereinafter: Company), who is authorised to make the present declaration, I hereby make the following declaration.

The Company declares that it is aware that in the course of their services provided for the University of Debrecen (registered seat: 4032 Debrecen, Egyetem tér 1; hereinafter: Controller), it has access to personal data processed by the Controller, and as such, the Company participates in the data processing activity in its capacity as processor.

The Company declares that it only processes personal data on the basis of the instructions of the Controller, and that it performs the instructions given by the Controller. If it wishes to depart from the Controller's instruction, or a provision of law overwrites the Controller's instruction, it shall give prior notice of this fact to the Controller.

The Company undertakes an obligation that in case it wishes to use another company or sole trader for the purpose of performing the contract between the Company and the Controller, it shall give prior notice of this fact to the Controller. If the Controller consents to the use of the company or sole trader, the Company shall ensure that they also make a declaration of similar content toward the Company.

The Company shall ensure that its employees – or in case of the use of another company or sole trader, the employees of such other company or sole trader – have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Company shall guarantee the appropriate level of security according to Article 32 of the GDPR, in line with the activities engaged by it.

In case of a personal data breach, the Company shall notify the Controller of this fact within 24 hours after learning about it. The Company shall have an obligation to cooperate with the Controller in the reporting of the personal data breach to the National Authority for Data Protection and Freedom of Information (NAIH), as well as the investigation of the same.

The Company agrees that, after the termination of the contract between the Controller and the Company, it shall, at the option of the Controller, erase all personal data or return the document containing the personal data to the Controller and delete all existing copies.

If the Company notices that an instruction of the Controller breaches the GDPR or any other provisions of law, the Company shall give written notice of this fact to the Controller.

[Place, date]

[Signature]

Annex 12

Data Processing Agreement

concluded by and between the University of Debrecen (registered seat: 4032 Debrecen, Egyetem tér 1, tax number: 19308667-4-09, group tax identification number: 17782218-5-09, EU VAT number: HU17782218, institute identifier: FI 17198, bank account number: ....., represented by: Prof. Dr. Zoltán Bács, rector; with respect to the present contract, pursuant to power of attorney no. RH/....., ... (hereinafter: Controller:

and ..... (data of the partner), hereinafter: Processor), under the following terms and conditions:

1. Definitions

1.1. Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2. EEA states: countries outside the EEA states (EU member states, as well as Iceland, Liechtenstein and Norway.

1.3. GDPR: Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation). The acronym GDPR, widely used in practice is derived from the English name of the regulation (General Data Protection Regulation).

1.4. NAIH: the National Authority for Data Protection and Freedom of Information (NAIH)

2. The Processor's compliance with the GDPR

The Processor warrants that is has expert-level knowledge, reliability and resources to implement the technical and organisational measures ensuring compliance with the requirements of the GDPR, including the safety of the processing.

3. The scope of the processing

The Controller shall use the Processor in connection with the following processing:

- the subject of the processing: the processing of personal data according to contract no. ..... concluded on ..... in the subject of .....
- the nature and the purpose of the processing: .....
- the duration of the processing: .....
- the scope of the processed data: .....

4. The Processor's general obligations

4.1. The processing of the personal data by the Processor shall take place in the framework of the present contract, limited to the extent that the Controller instructed the Processor, and only in connection with the service. The Processor shall process the personal data on behalf of the Controller.

4.2. If the transfer of the personal data becomes necessary for the provision of the service (including any form of data transfer, but especially transmission to a third country), the Processor may only do this with the prior consent of the Controller. Transmission to a third country shall also deem to include any cloud-based processing, if the provider of the cloud-based service cannot represent and warrant that they shall not perform and processing on the data transmitted for the purpose of processing.

4.3. The Processor may not process or use the personal data for any purpose beyond the extent expected and necessary for the performance of the services.

4.4. The Processor shall comply with all relevant provisions of Hungarian and EU law, as well as the requirements of the authorities. The Processor shall ensure all such forms of cooperation and support, and shall provide all such information that is required by the Controller in the interest of verifying its compliance with the relevant provisions of law and the performance of its obligations, as well as to be able to cooperate with the NAIH and to perform its instructions or decisions, while also keeping the deadlines imposed by the NAIH or the supervisory authority conducting the given proceeding.

4.5. The Processor shall only process the personal data on the basis of the Controller's written instructions, including the transmission of the personal data to a third country or an international organisation, except when the processing is required by a provision of EU or national law binding upon the Processor. In this case, the Processor shall notify the Controller of the given legal requirement prior to the processing of the data, except when such notification is prohibited by the given provision of law for important reasons of public interest.

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including on-site inspections, conducted by the Controller or another auditor mandated by the Controller.

4.6. The Processor warrants that the persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.7. Taking into account the state of the art in science and technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.8. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the the applicable law or other data protection provisions of the European Union or a Member State.

4.9. After the end of the provision of services relating to processing, the Processor shall, depending on the instruction of the Controller, erase or return to the Controller all the personal data, and shall erase existing copies of the same, unless Union or Member State law requires storage of the personal data. If a provision of EU or national law requires the Processor to retain the personal data, the Processor shall without delay, but in any case not later than within 5 business days after learning of such requirement, certify to the Controller, by way of sending a document evidencing the above, the continued retention of the personal data.

5. The use of sub-processors

5.1. The Processor may not use a sub-processor without the prior express authorisation of the Controller.

5.2. If the Processor, with the prior, express consent of the Controller, uses a sub-processor for the performance of certain specific processing activities on behalf of the

Controller, then the same data protection obligation shall be binding upon these sub-processors, by way of contracts, as imposed by the present contract, and especially in such a way that it should provide safeguards for the implementation of appropriate technical and organisational measures, in such a way that the processing should satisfy the requirements of the applicable law.

5.3. Only such sub-processors may be proposed whose suitability was properly supported or warranted by the Controller.

5.4. The Controller may, at any time, withdraw its consent to the use of sub-processors if such information comes into the possession of the Controller that calls into doubt the sub-processor's suitability.

6. The rules of maintaining contact and giving instructions

6.1. The Controller undertakes that, within 1 business day from the date when the present contract was concluded, it shall notify the Processor of the name, e-mail address and telephone number of the contact person (or contact persons) of the Controller. The contact person (or contact persons) of the Controller shall have the right to give instructions in connection with the processing, and the Processor shall be required to contact the contact person (or contact persons) with its comments. The Controller agrees to notify the Processor of any change in the above data within one business day.

6.2. The Processor undertakes that, within 1 business day from the date when the present contract was concluded, it shall notify the Controller of the name, e-mail address and telephone number of the contact person (or contact persons) of the Processor. Any instructions of the Controller in connection with the present contract shall be addressed to the contact person (or contact persons) of the Processor. The Processor agrees to notify the Controller of any change in the above data within 1 business day.

7. Reporting personal data breaches

7.1. Immediately after the occurrence of a personal data breach comes to its attention, or in any case within not more than 24 hours, the Processor shall notify the personal data breach to the Controller, and shall cooperate with the Controller in the course of notifying the competent supervisory authority.

7.2. In its notification given within 24 hours, the Processor shall cover, in particular, the following:

- the nature of the personal data breach (the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data).

- the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

7.3. If the Processor fails to notify the Controller within 24 hours, the Processor shall be required to inform the Controller concerning the cause of such delay.

7.4. The Processor shall immediately notify the Controller in connection with the personal data breach concerning the following, as soon as the circumstances of the above have been clarified:

- the detailed description of the personal data breach;
- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name of all data subjects concerned (or in case this is not possible, the number of the data subjects and the records/databases containing their personal data);
- the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8. Participation in the exercise of the data subject's exercise of rights

8.1. The Processor shall actively support the Controller in the performance of its obligation with respect to confirming whether or not the personal data pertaining to a specific data subject are being processed, and if so, providing access for the data subject to the personal data and information.

8.2. The Processor shall actively support the Controller in the performance of its obligation to:

- rectify (correct) any inaccurate personal data;
- supplement any deficient personal data;
- delete the personal data;
- restrict access if any of the following is not satisfied.

8.3. If the Controller receives a request from a data subject in accordance with Article 18 (1), point a) of the GDPR, at the instruction of the Controller, for the duration indicated in that instruction, the Processor shall restrict the processing of the data in the system, including in particular the temporary termination of access authorisation, except in the case of those who participate on the part of the Controller or the Processor in the handling of the request of the data subject.

8.4. If the Controller receives a request from a data subject in accordance with Article 18 (1), point b) to d) of the GDPR, at the instruction of the Controller, the Processor shall copy the personal data identified in the instruction of the Controller to a storage medium provided by the Controller, and such information shall be erased by the Processor from its system.

8.5. In case the Processor receives requests related to the exercise of the data subject's rights directly from data subjects, the Processor shall forward these requests, without delay, to the Controller, and may only reply to the data subject's request in case of the written consent of the Controller.

9. Liability

9.1. The Processor shall be liable for any and all damage arising from the breach of the obligations hereunder and of the provisions of the applicable law.

9.2. The Processor warrants that it shall provide compensation for all damage arising from the breach of the obligations hereunder and of the provisions of the applicable law.

Place and date: .....

On behalf of the Controller:	On behalf of the Processor:
.....	.....
<name of authorised representative>	Name of authorised representative:
<title of authorised representative>	<title of authorised representative>
University of Debrecen	<company name – if the contract is concluded with a company>

Legal countersigner:

.....

Annex 13

Controllers' Agreement

-

(registered seat: hereinafter: Controller 1),
and
-
(registered seat: -, hereinafter: Controller 2),

(the parties hereinafter jointly: Parties or Controller) concluded a retainer / service // other contract with each other on [day, month, year]. On the basis of this contract the Parties shall jointly perform all activities that include the processing of personal data, and therefore, the Parties shall be considered as joint controllers.

Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR) constitutes several new obligations for joint controllers; for example, pursuant to Article 26 of the GDPR, they need to conclude an agreement with each other. With a view to the above, the Parties conclude a controllers' agreement that sets forth their respective rights and obligations.

1. Compliance with the GDPR

The Parties warrant that they have expert-level knowledge, reliability and resources to implement the technical and organisational measures ensuring compliance with the requirements of the GDPR- including the safety of the processing.

2. The description of the joint data processing

2.1. The Parties shall engage in the following joint data processing:
a) the designation of the processing: -
b) the purpose of the processing: -
c) the duration of the processing: -
d) the scope of the data processed: the personal data are stored on a server operated by Controller 1.

2.2. In addition to the processing in subsection 2.1, the Parties shall also engage in the following data processing jointly:
a) the designation of the processing:
b) the purpose of the processing:
c) the duration of the processing:
d) the scope of the data processed: the personal data are stored on a server operated by Controller 1.

3. Performance of the obligation related to providing information in advance

3.1. The preparation of the privacy notice (information on data processing) according to Articles 13 or 14 shall be the obligation of Controller 1; however, before finalising the privacy notice, the consent of Controller 2 shall also be obtained.

3.2. The Controllers shall publish the privacy notice on the main page of its website.

4. The data subject's exercise of rights

4.1. It shall be the obligation of Controller 1 to perform the requests received in the course of the exercise of rights according to Articles 15 to 22 of the GDPR.

4.2. At the request of Controller 1, Controller 2 shall participate in the performance of the data subject's rights.

4.3. The data subject may submit his/her request to either Controller. The Parties shall forward to each other the data subject's requests within 3 business days.

5. The rules of maintaining contact

The Parties undertake that, within 1 business day from the date when the present contract was concluded, they shall notify each other of the names, e-mail addresses and telephone numbers of their respective contact persons. The Parties agree to notify each other of any change in the above data within one business day.

6. Reporting personal data breaches

The party noticing the personal data breach shall immediately notify this fact to the other party, and then take the necessary measures after due consultation.

7. Liability

7.1. The Parties agree that they shall not be entitled to the reimbursement of the costs incurred on the side of the other party, as well as costs arising from the performance of obligations under the present agreement or from provisions of EU or national laws.

7.2. The Parties shall be liable towards each other for all damage arising from the violation of the obligations hereunder or of the provisions of EU or national laws. The Parties agree that they shall compensate each other for all damage arising from the violation of the obligations hereunder or of the provisions of EU or national laws.

[Place, date]
[Signature]

Annex 14

Records of data transmissions

Serial no.	The name of the organisational unit performing the supply of the data (controller)	The time/frequency and manner of the transmission of personal data	The legal basis of the data transmission	The recipient of the transmitted data	The scope of the personal data transmitted	The scope of the data subjects	Other data as defined in the provision of law on data processing (the name and address of the requesting body/person; the purpose/legal basis/date and time of the request)	The security measures applied in the course of the data transmission	Name of the registering person, date of registration