Károli Gáspár University of the Reformed Church in Hungary

Privacy Policy

Pursuant to Act CCIV of 2011 on national higher education (hereinafter: National Higher Education Act), Act CXII of 2011 on the right of informational self-determination (hereinafter: Privacy Act) and the freedom of information and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: General Data Protection Regulation), the Senate of Károli Gáspár University of the Reformed Church in Hungary (hereinafter referred to as the University) adopts the following regulation on data management and data protection.

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose and scope of the Policy

(1) The purpose of this Policy is to establish the legal framework for the University's data management activities and to ensure compliance with the constitutional principles of data protection and data security, to prevent unlawful access, alteration and unauthorised disclosure of data.
(2) The scope of the Policy covers the data management and data processing of personal data carried out by all organisational units of the University.

Article 2

Basic concepts and principles

(1) For the purpose of this Policy
1. 'personal data' means any information relating to an identified or unidentified natural person ('data subject') on the basis of which the data subject can be identified, directly or indirectly, in particular by reference to an identifier (e.g. name, an identification number, location data, an online identifier) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. 'sensitive data' means all data belonging to the special categories of personal data revealing racial or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data and personal data concerning the sex life or sexual orientation of natural persons;
3. 'data concerning health' means any data concerning the data subject's physical, mental or psychological status, addictions and the circumstances of illness or death, the cause of death communicated by or about the subject data, or detected, examined, measured, interpreted or derived by the health care services; and any data relating to or affecting any of the aforementioned (e.g. behaviour, environment, occupation);
4. 'processing' means 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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

5. ‘data processing’ means the set of processing operations carried out by the processor acting on behalf of or under the instructions of the controller.

(2) For additional definitions not defined in this Policy, the provisions of the General Data Protection Regulation and the Privacy Act shall apply.

(3) The University will carry out its data processing activities in accordance with the principle of lawfulness, fairness and transparency, purpose limitation, data minimisation and storage limitation, accuracy and integrity and confidentiality. The University’s organisational units shall ensure that the University is able to demonstrate compliance with the principles and rules on data management (accountability principle).

Article 3

Data handling and processing

(1) The University is the controller of the data processed at the University. Processing is carried out through the authorized organisational units of the University.

(2) For data processing, the University may use a data processor who will carry out processing for the University on behalf of the controller, or, as the case may be, under the specific instructions of the controller. The University may only use a data processor who provides sufficient guarantees for the implementation of appropriate technical and organisational measures to ensure compliance with data protection rules and the protection of the rights of data subjects.

(3) The University may process data for other data controllers.

(4) The terms and conditions for data processing must be included in a written agreement which may also form part of another contract. Processing may also be carried out on the basis of legal provisions, in which case the legal provisions shall apply to the data processing relationship.

(5) The data processing agreement shall include at least

a) the subject-matter, duration, nature and purpose of the processing, the type of personal data and the categories of data subjects;

b) that, unless otherwise provided by law, the processor will process data in accordance with written instructions from the controller (including those communicated by electronic means) and the circumstances in which the instructions were given, such as the name of the organisational unit or person entitled to carry out the instruction;

c) the obligation for the processor to inform the controller without delay if he/she considers that any of the instructions breaches the data protection rules;

d) whether the processor is entitled to use an additional data processor, and if so, the obligation to provide information regarding the use or replacement of the additional data processor or change of processors and the circumstances in which the controller’s objection should be communicated;

e) that, if an additional data processor is used, the additional processor shall be subject to at least the same obligations and at most the same rights as the processor, and that the processor shall be fully liable for any infringement of the additional data processor;

f) that the processor shall take appropriate data security measures and, if necessary, a general description of the data security measures;

g) the rules on the information on data protection incidents and cooperation;

h) the rules on cooperation to ensure the rights of the data subject, in particular the rules on the technical and organisational measures which, as far as possible, will assist the controller to fulfil its obligation to respond the requests relating to the exercise of the rights of the data subject;

i) the rules for cooperation in the data protection impact assessment, if necessary;

j) a confidentiality obligation on behalf of the processor, whereby the processor ensures that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

k) the obligation that the processor deletes all personal data (including existing copies) or returns them to the controller, at the choice of the controller, after the end of the processing, unless otherwise provided by law;
l) that the processor makes available to the controller any information necessary to demonstrate compliance with the lawfulness of data processing and allow for audits, including on-site inspections, conducted by the processor;
m) that the processor makes available all information necessary to comply with the controller's legal obligations; and cooperates in the monitoring, inspection or audit of the processing;
n) where necessary, additional rights and obligations of the controller and the processor based on the agreement of the parties.

CHAPTER II

RULES ON DATA PROCESSING

Article 4

Purpose of processing

(1) The University processes personal data for purposes related to its operation, in particular for the purposes of higher education activities (teaching, research and artistic creative activities), employment, document management, IT services and information security, graduate tracking, marketing and direct marketing, the operation of dormitories, the operation of personal and property security facilities, library and archives services.
(2) The specific rules applicable to each processing operation are set out in Part VII. The University may define additional processing purposes, if the legal conditions for this are met.

Article 5

Legal basis for processing

(1) The University may process personal data if:
a) Processing is required by law or local government decree for the performance of a task carried out in public interest or in the exercise of official authority (mandatory processing). Such processing includes, in particular, processing related to higher education activities or employment.
b) Processing is required to comply with a legal obligation. Such processing includes, in particular, processing that is strictly necessary for the fulfilment of a legal obligation (e.g. provision of data).
c) The data subject has given consent to the processing in accordance with sections (3)-(5). Such processing includes, in particular, certain processing relating to the sending of newsletters based on voluntary subscriptions, participation in prize games or various events, voluntary completion of questionnaires.
d) Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into the contract. Such processing may, in particular, include processing of data necessary for the conclusion of a contract for a service provided by the university on a voluntary basis.
e) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
f) 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 the protection of personal data, in particular where the data subject is a child (procession based on the balance of interests).

(2) If the duration of the mandatory processing or the periodic review of its necessity is not specified by law, the University shall review at least every three years whether the processing is still needed for the purposes for which it is intended. The circumstances and results of this review shall be documented by the controller, kept for ten years, and made available to the National Authority for Data Protection and Freedom of Information (Hungarian abbreviation: NAIH), if necessary.

(3) The consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her. The subject data may withdraw its consent at any time.

(4) The processing with consent may only be carried out if the requirements of prior information (Article 8) are complied with and voluntariness can be demonstrated.

(5) Consent may be given in any form in which the data subject can be identified, to the extent required for processing, and the fact of consent is documented, in particular:

a) in writing (signed by the data subject);

b) by electronic means,

ba) following identification of the data subject by logging into the education administration system, where the fact of consent is recorded (logged),

bb) by a message sent by the data subject from an electronic email address registered by the University, provided that the message is recorded and kept without alteration, or

bc) by using at least an advanced electronic signature.

(6) The Data Protection Offices shall be consulted in writing in advance by the organisational unit carrying out the processing before the processing based on the balancing of interests is started. The performance and outcome of the balancing of interests shall be documents.

(7) Sensitive data may only be processed if one of the conditions referred to in Article 9 (2) of the General Data Protection Regulation is met, including transfers of data.

Article 6

Prior data protection impact assessment

(1) If a type of processing. in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedom of the data subjects, the University shall, prior to the processing, carry out an impact assessment on how the planned processing operations will affect the protection of personal data.

(2) A mandatory data protection impact assessment must be carried out in the case of:

a) a systematic monitoring of a publicly accessible area on a large scale, such as the use of electronic surveillance system (camera) that complies with these conditions;

b) processing large amounts of data concerning health or other sensitive data;

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

d) data management which are on the list of the National Authority for Data Protection and Freedom of Information (NAIH) requiring a mandatory data protection impact assessment.

(3) No data management impact assessment is required for processing based on law (mandatory processing), processing necessary to comply with legal obligations, and processing which is exempted from data protection impact assessment by the National Authority for Data Protection and Freedom of Information (NAIH).

(4) The head of the organisational unit concerned shall consult with the data protection officer on the need for a data protection impact assessment. The data protection impact assessment is carried out

by the organisational unit concerned, but the data protection officer provides advice upon request as regards the data protection impact assessment and monitors its performance.

(5) In the case of data processing operations carried out with external (in particular application) funding where a data protection impact assessment is mandatory, the data protection impact assessment should be carried out at the expense of these funds. The organisational unit preparing the application or external funding shall consult the University data protection officer on the need for a data protection impact assessment before submitting the application.

(6) The data protection impact assessment shall contain at least
   a) a systematic description of the envisaged processing operations and the purposes and legal basis of the processing; including, in the case of processing based on a balance of interests, the legitimate interest pursued by the controller;
   b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   c) an assessment of the risks to the rights and freedoms of data subjects; and
   d) the measures envisaged to address the risks, including safeguards and data security measures to demonstrate compliance with the law and this Policy, taking into account the legitimate interests of data subjects.

(7) The results of the completed data protection impact assessment shall be sent to the University's data protection officer who can comment on the impact assessment.

(8) If the data protection impact assessment concludes that the planned processing operation is likely to result in a high risk, in the absence of measures to reduce the risks, the University will consult with the National Authority for Data Protection and Freedom of Information (NAIH), through the data protection officer, before processing the personal data.

Article 7

Records of processing activities

(1) For the purpose of keeping records of data management activities at the University, records shall be kept of all processing under the authorization of this Policy. The draft records are prepared by the data protection officer. The final text of the records is approved by the Rector's Council.

(2) The records are kept by the University in electronic or paper format.

(3) Records of processing activities document the basic characteristics of data management for each processing operation in accordance with the law and university regulations. In particular:
   a) the name and contact details of the controller and its representative and the data protection officer;
   b) the name and a brief description of the processing;
   c) the name and contact details of the organisational unit carrying out the processing and the name of the head of the organisational unit;
   d) the purpose(s) of the processing;
   e) the legal basis for the processing;
   f) where the legal basis for the processing is a balancing of interests [Article 5 (1) f)], a description of the balancing of interests carried out and the results thereof;
   g) where the processing is based on law [Article 5 (1) a)-b)] or is subject to legal provisions, the relevant legal provisions;
   h) the categories and (estimated) number of data subjects;
   i) the categories of processed data;
   j) the method of processing (manually, computerised, mixed);
   k) the source of data (data subject or other data processing);
   l) a general description of data security measures;
   m) the period of retention, deletion, or the criteria for determining the duration;

n) if a processor is used, the name of the processor and further details of the processing or the availability of the processing agreement;
o) the contact details provided for the exercise of the rights of data subjects;
p) information on the external data transfers, in particular the recipients of the transfers, legal basis for the transfers and the scope of the data typically transferred;
q) information on transfers of data to third countries, if applicable.

(4) The following may be attached to the records of data processing:
a) if necessary for the given processing, the result of the completed data protection impact assessment and consultation with the National Authority for Data Protection and Freedom of Information (NAIH);
b) the text of the information relating to data processing;
c) the text of legal provisions on data processing.

(5) The records of processing activities should be reviewed as necessary, in particular in the event of any change (reorganisation) of the organisational unit carrying out the processing or in the case of a change in the basic circumstances of the processing. After the end of the processing, the master file shall be archived by the organisational unit which carried out the processing.

(6) If the University is a processor acting on behalf of another data controller, it shall keep records of processing activities. These records shall include:
a) the name and contact details of the University as data processor, and the name of its representative and the data protection officer;
b) the name(s) and contact details of the controller(s), on behalf of which the processor is acting, and the name and contact details of the controller(s) and the name and contact details of their data protection officer, if any;
c) the categories of processing activities carried out on behalf of the controller;
d) a general description of data security measures;
e) information on transfers to third countries, if applicable.

Article 8

Prior information

(1) Where personal data are collected by the University from the data subject, the University shall provide the data subject with basic information about the processing and the rights relating to the data subject before the processing begins. This includes in particular:
a) the name of the controller and the name and contact details of its representative and data protection officer;
b) the purpose(s) of the processing;
c) the legal basis for the processing;
d) if the legal basis for the processing is the consent of the data subject [Article 5 (1) c)], information that the consent may be withdrawn at any time which, however, does not affect the lawfulness of the processing carried out on the basis of the consent before its withdrawal;
e) if the legal basis for the processing is a balancing of interests [Article 5 (1) f)], the legitimate interests of the controller or a third party;
f) where applicable, the recipients of personal data and the categories of recipients;
g) where applicable, information on transfers to a third country;
h) the period for which the data will be stored or the time of their deletion, or the criteria for determining this period;
i) information on the data subject’s right to request from the controller access to, rectification, erasure or restriction of his/her personal data and to object to processing of such personal data, and to exercise the right to data portability;
j) the right to lodge a complaint with a supervisory authority;

k) information whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for entering into a contract, whether the data subject is obliged to provide the personal data and the possible consequences of not providing such data;
l) the existence of automated decision-making, including profiling, referred to in Article 22 of the General Data Protection Regulation, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
m) where the University intends to further process the personal data for the purpose other than that for which the personal data were collected, it shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in points f)-l).

(2) Where personal data have not been obtained from the data subject, the University shall provide the data subject with the following information within 30 days of the receipt of the data or at the time of contacting the data subject:
a) the information referred to in section (1);
b) the scope of the personal data processed;
c) from which source the personal data originate, and if applicable, whether the data came from publicly accessible sources.

(3) The information referred to in sections (1) and (2) shall be communicated to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, as a general rule, in writing, including by electronic means.

Article 9

The obligation of secrecy

(1) Employees carrying out data controlling or processing at the University are obliged to treat personal data they learn in the course of their work confidential and to keep it as a secret. Only persons who have made a declaration of confidentiality or are legally bound to confidentiality may be employed in a position involving data processing, data management and access to personal data.
(2) The obligation of secrecy shall apply without time limit.
(3) The obligation of professional secrecy does not apply to personal data the publication, disclosure or accessibility of which is required by law in the public interest (public interest data).

CHAPTER III

TRANSFER AND DISCLOSURE OF DATA

Article 10

General rules

(1) Transfer of data means making the data available to a specific third party, including the possibility of consulting or extracting the data. The transmission of data within the organisational system of the University as data controller, the transfer of data to a processor or the access of the data subject to his/her own personal data is not considered a data transfer.
(2) Transfers of data to a third country means data transfers to a country outside the member states of the European Economic Area (hereinafter: EEA).
(3) Disclosure is when the data is made available to anyone.

Article 11

Transfer of data within the institution

(1) Within the organisational system of the University, personal data may be transferred, to the extent and for the period necessary for the performance of the task, to the organisational units which need the data to carry out their tasks specified by law, university regulations or instructions (hereinafter: internal transfer of data).
(2) In the event of a dispute between the organisational unit responsible for data management and the organisational unit wishing to access the data, the competent manager of both organisational units shall decide on the dispute.
(3) Internal data transfers shall be carried out in such a way that the fact of the transfer, the names of the sending and receiving organisational units, the purpose (reason) and date of the transfer and, at the request of any organisational unit, the further circumstances of the transfer are recorded and can be retrieved electronically or on paper.

Article 12

Transfer of data based on external request

(1) A request received from a body or individual outside the University for a transfer of data within the EEA may only be fulfilled or personal data may only be transferred for other purposes if one of the conditions (legal basis) laid down in Article 5 (1) of the Policy exists. The possible legal basis or legal bases for the transfer of data or other circumstances of transfer shall be recorded in the recordings of processing for each processing operation.
(2) In the case of transfers from data processing based on consent, the consent must also explicitly cover data transfers. The provisions of Article 5 (3)-(5) shall apply to the consent accordingly.
(3) The provision of data based on law, in particular at the request of a court, police, prosecutor's office, bailiff or public administration body, as well as to the maintainer and the body responsible for the operation of the higher education information system shall be carried out by the head of the organisational unit responsible for data management with the notification of the data protection officer.
(4) Transfer based on a balancing of interests may only take place exceptionally, in particularly justified cases, after prior consultation with the data protection officer, if the legitimate conditions for the transfer are beyond doubt. The performance and outcome of the balancing of interests must be documented.
(5) In case of doubt, any organisational unit carrying out data management can contact the data protection officer in order to consult on the data transfer. The head of the organisational unit is obliged to give reasons for the provision or non-provision of data contrary to the opinion of the data protection officer.
(6) The head of the organisational unit concerned shall inform the Rector of the University about requests for data from the national security services. The Rector may appeal against such requests to the competent minister with a complaint without suspensive effect.
(7) The data subject or any other person or organisation may not be informed of any request or access to data from the national security services, including the fact of the request or consultation, and of the measures taken.
(8) Records must be kept of the fact and circumstances of the transfer, including at least:
    a) the person(s) involved in the transfer;
    b) the name of the organisational unit carrying out data management;
    c) the recipient of the transfer;
    d) the purpose and legal basis for the transfer,
    e) the date of the transfer.
(9) There is no need to keep records of transfers based on regular legal requirements, in particular those based on data reporting obligations to the Higher Education Information System or other similar state registers.

Article 13

Transfers to third countries or international organisations

(1) Data transfers to third countries or international organisations may only be made in accordance with the provisions of Chapter V of the Regulation. The provisions of Article 12 (8)-(9) shall apply to data transfers accordingly.
(2) In any event, the organisational unit responsible for data processing shall consult the data protection officer in advance on the existence of the legitimate conditions for the data transfer referred to in section (1).

Article 14

Disclosure of personal data

The provisions of Article 12 (1)-(5) shall apply to the disclosure of personal data processed at the University.

CHAPTER IV

SAFEGUARDING THE RIGHTS OF THE DATA SUBJECT

Article 15

Right of access

(1) The data subject shall have the right to obtain information on data processing relating to him/her, on the personal data processed, and to have access to the following information:
   a) the purposes of the processing;
   b) the categories of personal data concerned;
   c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; and, in case of the latter, the guarantees according to Article 46 of the General Data Protection Rules;
   d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   e) the additional rights of the data subject under Article 16-20;
   f) the right to lodge a complaint with a supervisory authority;
   g) where the personal data are not collected from the data subject, any available information as to their source;
   h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
(2) The controller shall provide the data subject with a copy of the personal data undergoing processing upon request. 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. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Article 16

Right to rectification

(1) The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him/her. Taking into account the purposes of processing, the data subject shall have the right to have incomplete personal data completed, by means of providing a supplementary statement.
(2) In exercising the right to rectify data, the University may request the presentation of appropriate supporting documents, if the type of the rectified data so requires.

Article 17

Right to erasure

(1) The controller shall have the obligation to erase personal data relating to the data subject upon the data subject's request without undue delay where one of the following grounds applies:
   a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for processing;
   c) the data subject objects to the processing pursuant to Article 20 and there are no overriding legitimate grounds for the processing,
   d) the personal data have been unlawfully processed;
   e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(2) Where the controller has disclosed the personal data and is obliged to erase them pursuant to section (1), he/she shall take reasonable steps, including technical measures, taking into account the available technology and the costs of implementation, to inform the other controllers which are processing the data to which the erasure request relates that the data subject has requested the erasure of the links to, or copy or replication of those personal data.
(3) It constitutes a legitimate restriction on the right to erasure and therefore sections (1) and (2) shall not apply where the processing is necessary:
   a) for exercising the right of freedom of expression and information;
   b) for compliance with a legal obligation under Union or Member State law that requires the controller to process personal data or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   c) for reasons of public interest in the area of public health in accordance with Article 9 of the General Data Protection Rules;
   d) where the right to erasure is likely to render impossible or seriously impair processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
   e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
   a) the data subject contests the accuracy of the personal data, in which case the restriction applies for a period of time enabling the controller to verify the accuracy of the personal data;
   b) the processing is unlawful and the data subject opposes the erasure of personal data and requests the restriction of their use instead;
   c) the controller no longer needs the personal data for the purposes of processing, but the data subjects requires them for the establishment, exercise or defence of legal claims; or

d) the data subject has objected to processing pursuant to Article 20 pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under section (1), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has requested the restriction of processing shall be informed by the controller before the restriction of processing is lifted.

Article 19

Right to data portability

(1) The data subject shall have the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where

a) the processing is based on consent or agreement pursuant to Article 5 (1) c-d) of this Policy; and

b) the processing is carried out by automated means.

(2) In exercising his/her right to data portability pursuant to section (1), the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible.

(3) The exercise of the right referred to in section (1) of this Article may not prejudice the right to erasure or oblivion or adversely affect the rights and freedoms of others.

Article 20

Right to object

(1) The data subject shall have the right to object, on grounds relating to his/her particular situation, at any time to processing of personal data concerning him/her which is based on point f) of Article 5 (1), including profiling based on those provisions. In that case, the controller may no longer process the personal data, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

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

(3) At the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

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

Article 21

Common rules on the exercise of data subjects' rights

(1) The University shall ensure the exercise of the data subject' rights upon request submitted to the competent administrator specified in the register of processing activities. Where the exercise of the

data subject's rights results in the disclosure of personal data, it may be exercised only with the identification of the data subject, in particular

a) in writing (signed by the data subject);
b) electronically, following the unique identification of the data subject (e.g. identification with the education administration system), provided that the fact of the access is recorded (logged);
c) by electronic mail from the electronic mail address of the data subject registered by the University, provided that the message can be recorded and stored without alteration;
d) orally (in person or by phone), provided that identification is ensured by means of an identification card, by personal acquaintance between the administrator and the data subject or by checking at least four identifiers, including, if available, the identifier used for the education administration system.

(2) The University may also ensure the data subject's rights by means of an electronic device providing direct access, rectification or erasure.
(3) The University shall inform the data subject of the measures taken in connection with the exercise of the rights specified in this Policy, without undue delay but no later than one month from the date of receipt of the data subject's request the latest. If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by another two months.
(4) The University shall inform all recipients of any rectification, erasure or restriction of processing to whom or with which the personal data have been disclosed, unless it proves impossible or requires a disproportionate effort. Upon request, the controller shall inform the data subject of these recipients.
(5) If the University considers that the request cannot be fulfilled, it shall inform the data subject, without delay but no later than one month from the date of receipt of the request, of the reasons for the failure to act, and of the possibility to lodge a complaint with the supervisory authorities or to exercise his/her right of judicial remedy.
(6) Any data subject whose personal data are processed under this Policy, may directly contact the data protection officer with a complaint relating to the processing of his/her personal data. The data protection officer shall investigate the complaint, inform the data subject of the outcome of the investigation and, if justified, initiate the necessary measures to be taken by the organisational unit responsible for the processing.

CHAPTER V

DATA SECURITY

Article 22

General requirements for data security

(1) The University shall implement appropriate technical and organisational measures to ensure that the University guarantees an adequate level of data security, including in particular the confidentiality, integrity, availability and resilience of processing systems and services, and the ability the restore the availability and access to personal data in a timely manner in the event of an incident.
(2) Specific data security measures shall be chosen by the University taking into account the current state of science and technology, the costs of implementation, the nature, scope, circumstances and purposes of the processing, and the risk to the rights and freedoms of natural persons, of varying likelihood and severity.
(3) In determining the appropriate level of security, explicit consideration should be given to the risks arising from the data processing, in particular accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Article 23

Data security measures

(1) The following measures shall be taken to ensure the security of manually processed (non-electronic, typically paper-based) personal data:
   a) Fire and property protection: Documents held in the archives must be stored in a lockable, dry room suitable for preserving the condition of the documents.
   b) Access protection: Only authorized administrators may access to documents in active permanent management. Personnel and payroll and employment files must be kept in a lockable room and lockable safe, student files in a lockable room and lockable filing cabinet, and other personal data must be kept at least in a lockable room.
   c) Archiving: Archiving must be carried out in accordance with the University's regulation on document management and disposal and the archiving plan.

(2) Detailed rules on the security of personal data processed by electronic means, including a procedure for the regular testing, assessment and evaluation of the effectiveness of data security measures, are determined in the University's Information Regulation.

Article 24

Procedure for data breaches

(1) 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(2) If any employee of the University suspects a data breach or is informed of a data breach by the processor, he/she shall immediately notify the head of the organisational unit responsible for the processing. The head of the organisational unit will decide whether the event is qualified as a data breach. The staff member of the organisational unit carrying out the processing shall record the circumstances of the data breach without delay, in particular:
   a) the nature of the 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;
   b) the likely consequences of the data breach;
   c) the measures taken or planned by the given organisational unit or proposed to other organisational units to remedy the breach, in particular measures to mitigate its possible adverse effects;
   d) measures that the data subject can take, where appropriate, to mitigate any adverse effects;
   e) the general data security measures taken prior to the data breach;
   f) the draft text of the notification to the data subject.

(3) The organisational unit carrying out the processing shall notify the data protection officer of the circumstances of the breach within 24 hours of the detection, and propose a classification of the seriousness of the breach which can be (i) minor, (ii) likely to result in a risk or (iii) likely to result in a high risk. If all the information is not available within 24 hours, he/she will provide as much information as possible.

(4) The data protection officer will form his/her position on the seriousness of the breach and the appropriate follow-up actions on the basis of the available information and, if necessary, ask further information from the organisational unit which may have more information about the breach. The organisational unit contacted will provide the additional information available within 24 hours.

(5) The head of the organisational unit responsible for processing decides on the seriousness of the breach, taking into account the opinion of the data protection officer. When
   a) the personal data breach is likely to result in a risk or a high risk to the rights and freedoms of natural persons, the University shall notify the National Authority for Data Protection and

Freedom of Information (NAIH) of the data breach through its data protection officer within 72 hours of the detection of the breach,

b) the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, or the cooperation of the data subject is necessary to mitigate the adverse effects of the breach, and no relevant legal exceptions apply, the University, with the involvement of the relevant organisational unit and the data protection officer, will ensure that the data subjects affected by the beach are informed.

(6) This information shall include at least
   a) the nature of the personal data breach and the personal data concerned;
   b) the name and contact details of the data protection officer, or where data concerning health is concerned, of the data protection officer responsible for data concerning health or contact person who can provide further information;
   c) information referred to in points b)-d) of section (2).

(7) The University, through the data protection officer, keep records of all data protection incidents regardless of their seriousness with the data content referred to in Article 24 (2)-(3).

(8) The organisational units carrying out data processing shall keep a list of the types of personal data breaches that are theoretically possible or have already occurred, and shall regularly inform the data protection officer thereof. In justified cases, and on the basis of the indication of the data protection officer the organisational units responsible for data processing, shall draw up an action plan to reduce the number and severity of personal data breaches.

CHAPTER VI

INTERNAL SUPERVISION SYTEM FOR DATA PROTECTION

Article 25

Tasks of the organisational units responsible for data management

(1) Compliance with the legal provisions and university regulations on data protection, in particular with the provisions of this Policy, shall be continuously monitored by the heads of the organisational units responsible for data processing in line with their managerial duties. In an infringement of law is detected, the head of the unit shall take immediate action to put an end to it.

(2) The head of any organisational unit may, if necessary, contact the data protection officer with questions concerning the management, processing and regulation of personal data.

Article 26

Designation of the data protection officer

(1) The Rector of the University shall designate or appoint a data protection officer to supervise the legal and regulatory provisions on data processing and to facilitate the enforcement of the rights of data subjects. The data protection officer may be designated or appointed if he/she has an adequate level of knowledge of the legal provisions and practices relating to the protection of personal data, in particular professional studies, practical experience or academic work in these fields.

(2) The data protection officer may also perform other tasks, provided that these tasks do not conflict. A task is incompatible if it involves taking substantive decisions concerning data processing.

(3) The data protection officer shall perform his/her duties directly and exclusively under the authority of the Rector, in a professionally independent manner, and shall not accept specific instructions.

(4) The data protection officer shall receive a regular monthly remuneration for his/her activities, and shall be provided with the necessary resources to maintain his/her professional knowledge.

(5) The work of the University's data protection officer is assisted by a data protection assistant under his/her professional guidance.

Article 27

Tasks of the data protection officer

(1) The data protection officer shall
   a) provide information and professional advice on the obligations under the data protection provisions, by taking a position in a specific case or by making recommendations on general issues;
   b) contribute to the preparation and review of data processing records;
   c) upon request, provide professional advice on the data protection impact assessment and monitor the implementation of the impact assessment;
   d) monitor compliance with data protection provisions (legislation and university regulations) in the order, at the intervals and in the areas determined by him/her;
   e) contribute to awareness-raising and training of staff involved in data processing operations, as well as to internal inspections (audits) concerning personal data;
   f) cooperate with the National Authority for Data Protection and Freedom of Information (NAIH) on data protection; and serve as a contact for the NAIH on data management issues and consult with the NAIH on any other matters as appropriate;
   g) facilitate the exercise of the rights of the data subject, in particular by investigating complaints and, if necessary, by initiating the necessary remedial actions;
   h) contribute to the drafting or modification of the University's Privacy Policy and other regulations relating to personal data.

(2) The data protection officer shall carry out his/her tasks, in accordance with the priorities he/she has established, having due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

(3) The University and the heads of all organisational units shall ensure that the data protection officer is involved in matters related to his/her duties in an appropriate and timely manner, including the opportunity to participate in meetings concerning such matters. In order to perform his/her duties, the data protection officer shall have the right to have access to the data processing operations and any related documents of all organisational units of the University. He/she may ask information orally or in writing from the head of the unit or its staff. The person providing information is responsible for its correctness. The data protection officer is bound by an obligation of confidentiality, without time limit, in connection with the personal data learnt during the investigation.

(4) In the event of a breach of the data protection rules, an infringement or threat of violation of the rules or other irregularities affecting personal data, the data protection officer shall make a proposal to eliminate, prevent or remedy the breach or irregularity. If necessary, the data protection officer will inform the senior manager of the organisational unit concerned or the senior management of the University of the situation and assist in restoring the lawful situation.

(5) The data protection officer shall draw up an annual report on his/her activities for the Rector no later than 31 January of the year following the year in question.

CHAPTER VII

RULES ON CERTAIN PROCESSING OPERATIONS

Article 28

Student data processing

(1) In connection with the applications and student status of applicants and students, the University shall carry out data processing in accordance with the Act on National Higher Education for the

purpose of the proper operation of the institution, the exercise of the rights and fulfilment of the obligations of applicants and students, the organisation of education and research, the keeping of records specified by law, the establishment, assessment and verification of entitlement to student benefits and graduate tracking.

(2) Student data management by faculty covers all students of the University. The organisational unit responsible for the processing of students' data is the Registrar's Office of the faculty or faculties, in which the student is studying. Student data may be transferred from the organisational unit responsible for data processing to other units in accordance with the provisions of Article 11 of the Policy.

(3) Detailed circumstances of student data processing are included in the data processing records kept for each processing in accordance with Article 7.

Article 29

Employment data management

(1) In connection with the application and employment relationship (assignment relationship) of job applicants, employees and contracted lecturers, the University shall carry out data processing in accordance with the Act on National Higher Education and the Labour Code for the purpose of the proper operation of the institutions, the exercise of employer's rights, the exercise of the rights and the fulfilment of obligations of lecturers, researchers and employees, the keeping of records required by law, and the establishment, assessment and verification of entitlement to employee benefits.

(2) The organisational unit responsible for employment data processing is the Directorate for Economic Affairs. Employment data may be transferred from the organisational unit responsible for data processing to other units in accordance with the provisions of Article 11 of the Policy.

(3) Detailed circumstances of employment data processing are included in the data processing records kept for each processing in accordance with Article 7.

Article 30

Data processing for marketing purposes

(1) The University shall carry out data processing for marketing purposes in order to encourage the use of its services and to promote and increase the reputation and visibility of the University and its activities, in particular in the area of student recruitment and enrolment.

(2) The organisational unit responsible for processing for marketing purposes is the PR and Marketing Group. Personal data processed for marketing purposes may be transferred from the organisational unit responsible for data processing to other units in accordance with the provisions of Article 11 of the Policy.

(3) Detailed circumstances of data processing for marketing purposes are included in the data processing records kept for each processing in accordance with Article 7.

Article 31

Data processing for the protection of persons and property

(1) The University processes personal data in the operation of the security system for the protection of persons and property (in particular electronic surveillance and access control system).

(2) The organisational unit responsible for data processing related to the operation of the security system is the Directorate for Economic Affairs. Personal data processed by the responsible organisational unit in the course of the operation of the security system may be transferred to other units in accordance with the provisions of Article 11 of the Policy.

(3) Detailed circumstances of data processing concerning the operation of the security system are included in the data processing records kept for each processing in accordance with Article 7.

Article 32

Additional data processing for the operation of the University

(1) The University processes data for the purpose of the proper operation of the institution, in particular in the context of document management, business administration and application processes, organisation of events and operation of IT systems.
(2) The organisational units processing data relating to document management are independent units as specified in the organisational and operational rules. Data relating to business processes are processed by the Directorate for Economic Affairs. Data related to application processes are managed by the faculties and the Rector's Office. Data in connection with the organisation of events are processed by the faculties and the PR and Marketing Group. Data for the operation of IT system are processed by the Directorate for Economic Affairs. Personal data may be transferred from the processing organisational units to other units in accordance with the provisions of Article 11 of the Policy.
(3) The detailed circumstances of data processing in connection with the operation of the University, including the organisational units responsible for each processing, are set out in the data processing records kept in accordance with Article 7.

Article 33

Final provisions

This Policy shall enter into force on the date following its adoption. Upon its entry into force, all previous rules on data processing shall cease to apply.

Budapest, 23 August 2019.

Prof. Dr. Péter Balla
Rector