Károli Gáspár University of the Reformed Church in Hungary

Privacy and Data Management Policy

(English translation of the regulation approved in Hungarian, The text version is effective as of May 23, 2025.)

The Senate of Károli Gáspár University of the Reformed Church in Hungary (hereinafter referred to as the University) hereby adopts this Privacy and Data Management Policy in accordance with Act CCIV of 2011 on National Higher Education (hereinafter referred to as the Higher Education Act), Act CXII of 2011 on the right of informational self-determination and freedom of information (hereinafter referred to as Infotv.), 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 Directive 95/46/EC of the European Parliament and of the Council of 24 October 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 referred to as the General Data Protection Regulation).

CHAPTER I

GENERAL PROVISIONS

Article 1. Purpose and scope of the policy

(1) The purpose of this policy is to define the legal framework for the University's data processing activities, to ensure compliance with the constitutional principles of data protection and data security requirements, and to prevent unauthorized access, alteration, and disclosure of data.

(2) The scope of the policy extends to all data processing and data handling involving personal data carried out by all organizational units of the University.

Article 2. Basic concepts and principles

(1) For the purposes of this policy

1. Personal data: any information relating to an identified or identifiable natural person [data subject] and any conclusions about the data subject that can be drawn from the data.

Personal data shall retain this quality during data processing until the relationship with the data subject can be re-established. The relationship with the data subject can be re-established if the data controller has the technical conditions necessary for re-establishment;

2. Data subject: any natural person identified or otherwise identifiable, directly or indirectly, on the basis of personal data. A person is considered identifiable if they can be identified, directly or indirectly, by reference to a name, an identification number, or one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity;

3. Special data: any data belonging to special categories of personal data, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, and personal data related to the sexual life or sexual orientation of a natural person;

4. Health data: data relating to the physical, mental, and mental state of the data subject, his or her pathological condition, as well as the circumstances of illness or death, the cause of death, communicated by him or her or by another person, or detected, examined, measured, imaged, or derived by the healthcare network; and any data that can be linked to or influence the above (e.g. behavior, environment, occupation);

5. Data processing: any operation or set of operations performed on personal data or data files, whether automated or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

6. Data processing (by the data processor): all data processing operations performed by a data processor acting on behalf of or on the instructions of the data controller.

(2) With regard to other terms not defined in this policy, the provisions of the General Data Protection Regulation and the Infotv. shall apply.

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

Article 3. Data processing and data handling

(1) The data controller for data processing carried out at the University is the University. Individual data processing operations are carried out by the University's authorized organizational units.

(2) The University may use a data processor for data processing, who shall process data for the University on behalf of the data controller, on its behalf and, where applicable, in accordance with its specific instructions. The University may only use data processors who provide adequate guarantees for the implementation of appropriate technical and organizational 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 conditions for data processing shall be laid down in a written agreement, which may form part of another contract. Data processing may also be carried out on the basis of other legal acts referred to in Article 28(3) of the General Data Protection Regulation, in which case the provisions of the legal act shall govern the relationship between the data processor and the data controller.

(5) The data processing agreement shall include at least

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

b) unless otherwise provided by law, that the data processor shall carry out the data processing in accordance with the written instructions (including those communicated electronically) of the data controller, as well as the circumstances of the instructions, such as the name of the organizational unit or person authorized to give instructions;

c) that the data processor shall immediately inform the data controller if it considers that any of its instructions violate data protection rules;

d) whether the data processor is entitled to engage additional data processors and, if so, the information obligations relating to the engagement or replacement of additional data processors and the circumstances in which the data controller's objections must be communicated;

e) if additional data processors are used, the additional data processors shall be subject to at least the same obligations and enjoy no more rights than the data processor, and that the data processor shall be fully liable for any infringements committed by the additional data processors;

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

g) the rules on notification and cooperation in the event of a data breach;

h) the rules for cooperation in ensuring the rights of the data subject, in particular the rules on technical and organizational measures to assist the data controller, to the extent possible, in responding to requests related to the exercise of the data subject's rights;

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

j) the confidentiality obligation of the data processor, whereby the data processor ensures that persons authorized to process personal data undertake a confidentiality obligation or are subject to an appropriate confidentiality obligation under law;

k) the obligation of the data processor to delete all personal data (including existing copies) after the end of the data processing in accordance with the decision of the data controller, unless otherwise provided by law;

l) that the data processor shall make available to the data controller all information necessary to demonstrate the lawfulness of the data processing and to enable the data controller to carry out checks, including on-site inspections;m) that the data processor shall make available all information necessary for the data controller to comply with its legal obligations; and shall cooperate in the monitoring, on-site inspection or audit of the data processing;

n) if necessary, based on an agreement between the parties, the additional rights and obligations of the data controller and the data processor.

CHAPTER II.

RULES OF DATA PROCESSING

Article 4. Purpose of data processing

The University processes personal data for purposes arising in connection with its operations, in particular for the purposes of higher education (teaching, scientific research and artistic creation), employment, document management processes, the provision of IT services and the fulfilment of information security requirements, graduate career tracking, marketing and direct business acquisition

(direct marketing), the operation of dormitories, the operation of devices serving personal and property security, and library and archival services.

(2) Specific rules for individual data processing are contained in Chapter VII. of this policy, in the applicable legislation governing the specific data processing, and in other regulations of the University. The University may specify additional data processing purposes if the legal conditions are met.

Articla 5. Legal basis for data processing

(1) The University may process personal data if:

a) Data processing is required by law or municipal regulation for the performance of a task carried out in the public interest or in the exercise of official authority (mandatory data processing). Such data processing includes, in particular, data processing related to higher education activities or employment.

b) Data processing is necessary for the fulfillment of a legal obligation. Such data processing includes, in particular, data processing that is absolutely necessary for the fulfillment of an obligation prescribed by law (e.g., data reporting).

c) The data subject has given his or her consent to the data processing in accordance with paragraphs (3)-(5). Such data processing includes, in particular, certain data processing related to the sending of newsletters based on voluntary subscription, participation in prize games or various events, and the voluntary completion of questionnaires.

d) The data processing is necessary for the performance of a contract to which the data subject is party or for taking steps at the request of the data subject prior to entering into a contract. Such data processing may include, in particular, data processing necessary for the conclusion of a contract in the course of a freely available service offered by a university.

e) Data processing is necessary for the protection of the vital interests of the data subject or of another natural person.

f) Data processing is necessary for the purposes of the legitimate interests pursued by the data 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 particular where the data subject is a child (data processing based on legitimate interests).

(2) If the period for which the processing is necessary or the periodic review of the necessity of processing is not specified by law, the University shall review at least every three years whether the processing is still necessary for the purposes for which the data were collected. The circumstances and results of this review shall be documented by the data controller, retained for ten years and made available to the National Authority for Data Protection and Freedom of Information (NAIH) upon request.

(3) Consent is 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. The data subject may withdraw his or her consent at any time.

(4) Data processing may only be carried out on the basis of consent if the requirements for prior information (Section 8) are met and the voluntary nature of the consent can be verified.

(5) Consent may be given in any form which allows the data subject to be identified to the extent necessary for the processing and which provides for the recording of the fact that consent has been given, in particular:

a) in writing (with the signature of the data subject);

b) electronically,

ba) after identification of the data subject by logging into the study system, provided that the fact of consent is recorded (logged),

bb) in a message sent from the electronic address registered by the University for the data subject, provided that the message is recorded and stored without alteration, or

bc) using at least an advanced electronic signature.

(6) Before commencing data processing based on legitimate interests, the organizational unit performing the data processing shall consult with the data protection officer in writing in advance. The balancing of interests and its results shall be documented.

(7) Special data may only be processed, including transferred, if one of the conditions set out in Article 9(2) of the General Data Protection Regulation is met.

Article 6. Data protection impact assessment

(1) Where a new data processing operation is likely to result in a high risk to the rights and freedoms of data subjects, in particular due to the nature, scope, context, or purposes of the processing,

the University shall, prior to the processing, carry out an impact assessment to determine how the planned processing operations will affect the protection of personal data. A mandatory data protection impact assessment shall be carried out:

a) in the case of large-scale, systematic monitoring of public places, such as the use of electronic surveillance systems (cameras) that meet these conditions;

b) processing of large amounts of health and other special data;

c) systematic evaluation of certain personal characteristics of natural persons based on automated processing, including profiling, which produces legal effects concerning the natural person or similarly significantly affects the natural person;

d) in the case of data processing operations included in the NAIH's list of data processing operations subject to mandatory data protection impact assessment.

(3) No data protection impact assessment shall be carried out in the case of data processing based on law (mandatory) and data processing necessary for the fulfillment of a legal obligation, as well as in the case of data processing included in the NAIH's list of data processing operations exempt from data protection impact assessment.

(4) The head of the organizational unit concerned shall consult with the data protection officer on the necessity of a data protection impact assessment. The data protection impact assessment shall be carried out by the organizational unit concerned, but the data protection officer shall, upon request, provide professional advice on the data protection impact assessment and monitor its performance.

(5) In the case of data processing from external sources (in particular from tenders) where a data protection impact assessment is mandatory, the data protection impact assessment shall be carried out at the expense of those sources. The organizational unit preparing the application or the involvement of external resources shall seek the opinion of the university data protection officer on the necessity of a data protection impact assessment prior to submitting the application.

(6) The impact assessment shall cover at least

a) a systematic description of the planned data processing operations and an explanation of the purposes and legal basis of the data processing, including, in the case of data processing based on a balancing of interests, the legitimate interests pursued by the data controller;

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

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

d) the measures taken to address those risks, including the safeguards and data security measures to ensure compliance with the law and this policy, taking into account the legitimate interests of the data subjects.

(7) The results of the impact assessment shall be sent to the university data protection officer, who may comment on the impact assessment.

(8) If the data protection impact assessment finds that the planned data processing would actually pose a high risk in the absence of measures to mitigate the risks, the University shall consult with the NAIH with the assistance of the data protection officer prior to the processing of personal data.

Article 7. Records of data processing activities

(1) For the purpose of recording data processing activities carried out at the University, a data processing record shall be kept for all data processing activities, as authorized by this policy. The records shall be kept by the data protection officer.

(2) The register shall be kept by the University in electronic or paper form.

(3) The register of data processing activities shall document the basic characteristics of each data processing operation within the framework of the law and university regulations. These include, in particular:

a) the name and contact details of the data controller and, where applicable, the name and contact details of the joint data controller, the data controller's representative and the data protection officer;

b) the purposes of the data processing;

c) a description of the categories of data subjects and the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;

e) where applicable, information on the transfer of personal data to a third country or an international organization, including the identification of the third country or international organization and, in the case of a transfer pursuant to the second subparagraph of Article 49(1), a description of the appropriate safeguards;

f) where possible, the time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organizational measures referred to in Article 32(1).

(3) The following may be attached as annexes to the records of data processing operations:

a) where necessary for the data processing operation in question, the results of the data protection impact assessment carried out and the outcome of the consultation with the NAIH;

b) the information notice relating to the data processing operation;

c) the text of the legal provisions governing the data processing operation.

(4) The records of data processing activities shall be reviewed as necessary, in particular in the event of changes (reorganization) affecting the organizational unit responsible for data processing or in the event of a change in the fundamental circumstances of data processing.

(5) If the University acts as a data processor on behalf of another data controller, it shall keep a record of its data processing activities. This record shall include:

a) the name and contact details of the University as data processor, as well as the name of its representative and data protection officer;

b) the name and contact details of the data controller(s) on whose behalf the data processor is acting, as well as the name and contact details of the representative of the data controller(s) and, where applicable, the data protection officer;

c) the categories of data processing activities carried out on behalf of the data controllers;

d) a general description of the data security measures;

e) where applicable, information on the transfer of data to third countries.

Article 8. Information providing

(1) If the University collects personal data from the data subject, the data subject shall be provided with basic information on the data processing and their rights prior to the commencement of the data processing. Such information shall include, in particular:

a) the name of the data controller and the name and contact details of its representative and data protection officer;

b) the purpose(s) of the data processing;

c) the legal basis(es) for the data processing;

d) if the legal basis for the data processing is the consent of the data subject [Section 5 (1) c)], information that the consent may be withdrawn at any time, but that this does not affect the lawfulness of the data processing carried out on the basis of the consent prior to its withdrawal;

e) if the legal basis for data processing is a balancing of interests [Section 5 (1) f)], the legitimate interests of the data controller or a third party;

f) where applicable, the recipients of the personal data or categories of recipients;

g) where applicable, information on the transfer of data to a third country;

h) the time limit for which the data will be stored or the criteria used to determine the time limit;

i) information on the data subject's right to request from the data controller access to personal data concerning him or her, rectification or erasure of such data, restriction of processing, and to object to the processing of such personal data, as well as the right to data portability;

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

k) information that the provision of personal data is based on a legal or contractual obligation or is a prerequisite for entering into a contract, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to do so;

l) in the case of automated decision-making (and profiling) in accordance with Article 22 of the General Data Protection Regulation, the fact that such processing is carried out, the logic involved, and meaningful information about the significance of such processing and the envisaged consequences of such processing for the data subject;

m) if the University intends to further process personal data for purposes other than those for which they were collected, it shall inform the data subject of this different purpose and of all relevant information referred to in points f) to l) prior to such further processing.

(2) If the University does not collect personal data from the data subject, the data subject shall be informed, at the latest within 30 days of receipt of the data or when the data subject is contacted, of:

a) the information specified in paragraph (1);

b) the scope of the personal data processed;

c) the source of the personal data and, where applicable, whether the data are obtained from publicly available sources.

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

Article 9. Confidentiality

Employees of the University who are involved in data processing or data handling shall treat personal data obtained in the course of their work as confidential and keep it secret. Only persons who have signed a confidentiality agreement or are bound by law to maintain confidentiality may be employed in positions involving data processing, data handling or access to personal data.

(2) The confidentiality obligation shall remain in force indefinitely.

(3) The confidentiality obligation shall not apply to personal data whose disclosure, disclosure or accessibility is required by law in the public interest (data of public interest).

CHAPTER III

DATA TRANSFER AND DISCLOSURE TO THE PUBLIC

Article 10. General rules

(1) Data transfer means making data available to a specific third party, including allowing access to the data or making extracts from it.

Data transfer does not include the transfer of data within the organizational system of the University as a data controller, the transfer of data to a data processor, or the transfer of data to the data subject. Data transfer within the organizational system of the University as data controller, the transfer of data to a data processor, and the access of the data subject to his or her own personal data shall not be considered data transfer.

(2) Data transfer to a third country means the transfer of data to a country outside the European Economic Area (hereinafter referred to as the EEA).

(3) Disclosure means making the data available to anyone.

Article 11. Data transfer within the institution

(1) Within the organizational system of the University, personal data may be transferred to an organizational unit that needs the data to perform its tasks to the extent and for the duration necessary to perform its tasks as specified in the law, university regulations, or instructions (hereinafter referred to as internal data transfer).

(2) If a dispute arises between the data controller and the organizational unit wishing to access the data in connection with the performance of a task, the dispute shall be settled by the manager responsible for both organizational units.

(3) Internal data transfer shall be carried out in such a way that the fact of the transfer, the name of the sending and receiving organizational units, the purpose (reason) and date of the transfer, and, at the request of any organizational unit concerned, any further circumstances of the transfer are recorded electronically or on paper and can be retrieved.

Article 12. Data transfer based on external requests

(1) Requests for data transfer within the EEA from bodies outside the University or from private individuals may only be complied with, and personal data may only be transferred for other purposes, if one of the conditions (legal basis) set out in Section 5 (1) of this Regulation is met. The possible legal basis or legal bases for data transfer and other circumstances of data transfer shall be recorded in the register of the data controller for each data processing operation.

(2) In the case of data transfer based on consent, the consent must expressly cover the transfer of data. The provisions of Sections 5 (3)-(5) of this Regulation shall apply mutatis mutandis to consent.

(3) Data transfer based on law, in particular at the request of a court, the police, the public prosecutor's office, court enforcement officers or state administrative bodies, as well as data provision 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 organizational unit responsible for data processing, with the simultaneous notification of the data protection officer.

(4) Data transfer based on a balancing of interests may only take place in exceptional, particularly justified cases, after prior consultation with the data protection officer, if the conditions for the lawfulness of the data transfer are met beyond any doubt. The balancing of interests and its results shall be documented.

(5) In case of doubt, any organizational unit processing data may consult the data protection officer for consultation on data transfer. The head of the organizational unit shall justify any data provision that is performed or not performed contrary to the opinion of the data protection officer.

(6) The head of the organizational unit concerned shall inform the rector of the University of any requests for data from the national security services. The rector may lodge a complaint with the competent minister against such requests, which shall not have suspensive effect.

(7) The person concerned or other persons or organizations may not be informed of requests from national security services for access to data, including the fact of the request or access, or of the measures taken.

(8) A record shall be kept of the fact and circumstances of the data transfer, which shall include at least:

a) the person(s) concerned by the data transfer;

b) the name of the organizational unit responsible for data processing;

c) the recipient of the data transfer;

d) the purpose and legal basis of the data transfer;

e) the date of the data transfer;

(9) No data transfer register shall be kept for data transfers based on legal obligations, regular data transfers, in particular data transfers to higher education information systems or other similar state registers.

Article 13. Data transfer to third countries or international organizations

(1) Data transfers to third countries or international organizations may only take place in accordance with the provisions of Chapter V of the Regulation. Paragraphs (8) and (9) of Section 12 shall apply mutatis mutandis to data transfers.

(2) The organizational unit responsible for data processing shall in all cases consult the data protection officer in advance on the existence of the legal conditions for data transfer set out in paragraph (1).

Article 14. Disclosure of personal data

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

CHAPTER IV

ENSURING THE RIGHTS OF DATA SUBJECTS

Article 15. Right of access

(1) The data subject shall have the right to obtain information about the fact that data relating to him or her are being processed, about the personal data that are being processed, and shall have the right to access the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations; and, in the case of the latter, the guarantees provided for in Article 46 of the General Data Protection Regulation;

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 further rights of the data subject set out in Sections 16-20;

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

g) where the data have not been 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 significant effects and the significance and the envisaged consequences of such processing for the data subject.

(2) The data controller shall provide the data subject with a copy of the personal data undergoing processing upon request. The data controller may charge a reasonable fee based on administrative costs for any additional copies requested by the data subject. If the request was submitted electronically, the information shall be provided in a widely used electronic format, unless the data

subject requests otherwise. 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 or her. Taking into account the purposes of the processing, the data subject shall also have the right to request the completion of incomplete personal data by providing the necessary supplementary information.

(2) When exercising the right to rectification, the University may request the presentation of appropriate supporting documents if the type of data rectified so justifies.

Article 17. Right to erasure

(1) The data controller shall, at the request of the data subject, erase personal data concerning the data subject without undue delay if any of the following grounds apply:

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 there is no other legal basis for the processing;

c) the data subject objects to the processing pursuant to Section 20 and there are no overriding legitimate grounds for the processing;

d) the personal data has been unlawfully processed;

e) the personal data must be erased in order to comply with a legal obligation to which the controller is subject under Union or Member State law;

(2) If the data controller has made the personal data public and is obliged to erase it pursuant to paragraph (1), it shall take reasonable steps, taking into account available technology and the cost of implementation, to – including technical measures – to inform other controllers which are processing the personal data that has been made public and which is subject to the erasure request, of the erasure of the personal data or of the link to the personal data or of the fact of the erasure of the personal data or of the fact of the erasure to the data subject.

(3) The right to erasure is subject to a legitimate restriction and therefore paragraphs 1 and 2 shall not apply where processing is necessary:

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

b) for compliance with a legal obligation to which the controller is subject under Union or Member State law requiring the processing of 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) in accordance with the relevant paragraphs of Article 9 of the General Data Protection Regulation

on grounds of public interest in the area of public health;

d) if the right to erasure would render impossible or seriously impair

the archiving for public interest purposes, scientific or historical research purposes or

statistical purposes; or

e) for the establishment, exercise or defense 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 accuracy of the personal data is contested by the data subject, in which case the restriction shall apply for a period enabling the controller to verify the accuracy of the personal data;

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

;

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

d) the data subject has objected to the processing pursuant to Article 20; in this case, the restriction shall apply for a period no longer than that required to determine whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing is restricted pursuant to paragraph (1), such personal data shall, with the exception of storage, only be processed with the consent of the data subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) The data controller shall inform the data subject who requested the restriction of the data processing about the lifting of the restriction.

Article 19. Right to data portability

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the data controller, in a structured, commonly used and machine-readable format, and shall 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 legal basis for the processing is consent or a contract as defined in Section 5 (1) c-d) of this policy; and

b) the processing is carried out by automated means.

(2) When exercising the right to data portability pursuant to paragraph (1), the data subject shall have the right to request the direct transfer of personal data between controllers, where technically feasible.

(3) The exercise of the right referred to in paragraph (1) of this Article shall not affect the right to erasure or to be forgotten; nor shall it 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 or her particular situation, at any time to processing of personal data concerning him or her which is based on point (f) of paragraph 1 of Article 5 of this Regulation, including profiling based on that provision.

(2) If any employee of the University suspects a data protection incident or receives a report of a data protection incident from the data processor, they shall immediately notify the head of the organizational unit responsible for data processing. The head of the organizational unit shall decide whether the incident constitutes a data protection incident. The employee of the organizational unit performing the data processing shall immediately record the circumstances of the incident, in particular:

a) the nature of the incident and, where possible, the scope and (estimated) number of data subjects and the scope of personal data concerned;

b) the likely consequences of the incident;

c) the measures taken or planned by the organizational unit to remedy the incident, or recommended to other organizational units, in particular those aimed at mitigating any adverse consequences;

d) measures that may be taken by the data subject to mitigate any adverse consequences;

e) general data security measures in place prior to the incident;

f) where applicable, the draft text of the information to be provided to the data subject.

(3) The head of the organizational unit responsible for data processing shall inform the data protection officer of the circumstances of the incident within 24 hours of its detection and propose a classification of the severity of the incident, which may be

(i) insignificant,

(ii) incident likely to pose a risk, or

(iii) incident likely to pose a high risk. If all information is not available within 24 hours, the head shall provide as much information as possible.

(4) Based on the available information, the data protection officer shall form an opinion on the severity of the incident and on any further measures to be taken, and, if necessary, request further information from the organizational unit that is likely to have further information about the incident. The organizational unit contacted shall provide the additional information available within 24 hours.

(5) The head of the organizational unit responsible for data processing shall decide on the severity of the incident, taking into account the opinion of the data protection officer. If

a) the data breach is likely to result in a risk or high risk to the rights and freedoms of natural persons, the University shall notify the NAIH of the data breach within 72 hours of becoming aware of it, through the data protection officer.

b) the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons, or the cooperation of the data subject is necessary to mitigate the adverse consequences of the incident, and there are no relevant legal exceptions, the University shall ensure that the persons affected by the incident are informed, with the involvement of the organizational unit concerned and the data protection officer.

This information shall include at least

a) the nature of the incident and the scope of the personal data concerned;

b) the name and contact details of the data protection officer or, in the case of health data, the health data protection officer or the contact person providing further information;

c) the information specified in points b) to d) of paragraph (2).

(7) The University shall, through the data protection officer, keep a record of all data protection incidents, regardless of their severity, containing the information specified in Section 24 (2)-(3).

(8) The organizational units responsible for data processing shall keep a list of the types of data protection incidents that are theoretically possible and those that have actually occurred, and shall regularly inform the data protection officer thereof. Where justified, and at the request of the data protection officer, the organizational units performing data processing shall draw up an action plan to reduce the number and severity of data protection incidents.

CHAPTER VI

INTERNAL DATA PROTECTION SUPERVISION SYSTEM

Article 25. Tasks of the organizational units performing data processing

(1) The heads of the organizational units performing data processing shall, in accordance with their managerial duties, continuously monitor compliance with the legal provisions and university regulations relating to data protection, in particular the provisions of this policy. If the head of the unit detects a violation of the law, he or she shall take immediate action to remedy it.

(2) The head of any organizational unit may consult the data protection officer on any issues relating to the processing, handling or regulation of personal data.

Article 26. Appointment of the data protection officer

(1) In order to supervise compliance with the legal and regulatory requirements relating to data processing and to facilitate the enforcement of the rights of data subjects, the Chancellor of the University shall appoint or designate a data protection officer. The data protection officer shall be appointed or commissioned from among persons who have an adequate level of knowledge of the

legal requirements and legal practice relating to the protection of personal data, in particular through specialized studies, practical experience or academic work in this field.

(2) The data protection officer may also perform other tasks, provided that these tasks are not incompatible. Tasks that involve making substantive decisions relating to data processing are incompatible.

(3) The data protection officer shall perform his or her duties directly and exclusively under the authority of the chancellor, independently in a professional capacity, and shall not accept specific instructions.

(4) The data protection officer shall receive a monthly salary for his or her activities, and the necessary resources shall be provided to maintain the expert knowledge of the university data protection officer.

(5) The university data protection officer shall be assisted in his or her work by a data protection assistant working under his or her professional supervision.

Article 27. Tasks of the data protection officer

(1) The data protection officer

a) provides information and professional advice on obligations under data protection provisions, including issuing opinions on specific cases or recommendations on general issues;

b) participates in the preparation and review of data processing records;

c) provides professional advice on data protection impact assessments upon request and monitors the performance of such assessments;

d) monitors compliance with data protection provisions (legislation and university regulations) at intervals and in areas determined by him or her;

e) contributes to raising awareness and training of staff involved in data processing operations, as well as internal investigations (audits) involving personal data;

f) cooperates with the data protection authority (NAIH); and acts as a point of contact for the NAIH in matters relating to data processing and consults with it on any other issues, as appropriate;

g) facilitates the exercise of the rights of data subjects, in particular by investigating complaints from data subjects and, where necessary, initiating the necessary measures to remedy the situation;

h) participates in the drafting or amendment of the university's data protection policy and other policies relating to personal data;

(2) The data protection officer shall perform his or her tasks in accordance with the priorities he or she has set, taking into account the risks associated with data processing operations and the nature, scope, context and purposes of the data processing.

(3) The University and the heads of all organizational units shall ensure that the data protection officer is involved in matters relating to his or her tasks in an appropriate and timely manner, including the opportunity to participate in discussions on such matters. In order to perform his or her duties, the

University Data Protection Officer shall have the right to inspect data processing operations and any related documents at all organizational units of the University. He or she may request information from the head of the unit and his or her staff, either verbally or in writing. The person providing the information is responsible for its accuracy. The data protection officer is bound by confidentiality regarding any personal data obtained during his or her investigation, without any time limit.

(4) In the event of a breach of data protection rules, a violation of the law or a risk of a breach of the rules, or any other irregularity affecting personal data, the data protection officer shall make a proposal to remedy the breach or violation of the rules or to prevent or remedy the irregularity. If necessary, the data protection officer shall inform the head of the superior organizational unit of the organizational unit concerned and the senior management of the University of the situation and shall provide assistance in restoring the lawful state of affairs.

(5) The data protection officer shall prepare an annual report on his or her activities for the chancellor by January 31 of the year following the year in question.

CHAPTER VII

RULES ON SPECIFIC DATA PROCESSING OPERATIONS

Section 28

Processing of students' data

(1) The University shall process the personal data of applicants and students in connection with their application and student status for the purposes of the proper functioning of the institution, the exercise of the rights and fulfillment of the obligations of applicants and students, the organization of education and research, the maintenance of records specified by law, the determination, assessment and verification of eligibility for student benefits, and the career tracking of graduates.

(2) Student data processing is broken down by faculty and covers all students of the University. The organizational unit responsible for processing student data is the Study Department of the faculty or faculties where the student is enrolled. Student data may be transferred from the organizational unit performing data processing to other organizational units in accordance with the provisions of Section 11 of the Regulations.

(3) The Education Directorate shall be considered the data controller during the student evaluation of teaching (OMHV). Personal data shall be processed in accordance with the detailed rules set out in the University's Organizational and Operational Regulations. The organizational unit responsible for data processing shall ensure that the evaluated lecturers cannot identify the students who evaluated them (anonymization).

(4) The detailed circumstances of student data processing are set out in the relevant regulations of the University, as well as in the applicable legislation governing the specific data processing and in the data processing information notices prepared on the basis thereof.

Article 29. Employment data processing

(1) The University processes the personal data of job applicants, employees, and commissioned lecturers in connection with their application or employment relationship (commissioned legal relationship) for the purposes of the proper functioning of the institution, the exercise of employer's rights and the exercise of the rights and fulfillment of the obligations of lecturers, researchers and employees, the keeping of records specified by law, and the determination, assessment and verification of entitlement to employee benefits.

(2) The organizational unit responsible for labor data processing is the HR Directorate of the Rector's Office. Labor data may be transferred from the organizational unit responsible for data processing to other organizational units in accordance with the provisions of Section 11 of the Regulations.

(3) The detailed circumstances of labor data processing are contained in the relevant regulations of the University, as well as in certain applicable laws governing the specific data processing and in the data processing information prepared on the basis thereof.

Section 30. Data processing for marketing purposes

(1) The University shall process data for marketing purposes in order to promote the use of its services and to popularize and raise awareness of the University's name and activities, in particular in the areas of student recruitment and enrollment.

(2) The organizational unit responsible for data processing for marketing purposes is the Public Relations and Communications Directorate of the Rector's Office. Personal data processed for marketing purposes may be transferred from the organizational unit responsible for data processing to other organizational units in accordance with the provisions of Section 11 of the Regulations.

(3) The detailed circumstances of data processing for marketing purposes are set out in

the relevant regulations of the University, as well as in the applicable laws governing the specific data processing and in the data processing notices prepared on the basis thereof.

Section 31. Data processing for personal and property protection purposes

(1) The University processes personal data in the course of operating a security system (in particular an electronic surveillance system and an electronic access control system) for the purposes of personal and property protection.

(2) The organizational unit responsible for processing data related to the operation of the security system is the Facility Management Department of the Chancellor’s Office. Personal data processed by the organizational unit responsible for data processing in connection with the operation of the security system may be transferred to other organizational units in accordance with the provisions of Section 11 of the Regulations.

(3) The detailed circumstances of data processing related to the operation of the security system are set out in Section 32 of these Regulations, the relevant regulations of the University, and the applicable laws governing the specific data processing, as well as in the data processing information notices prepared on the basis thereof.

.

Section 32. Special rules relating to property protection camera systems

(1) The University operates electronic surveillance systems (property protection camera systems) on the premises it manages.

(2) The purpose of operating the systems specified in paragraph (1) as a data processing activity is to ensure the security of the real estate used by the University and subject to surveillance, to protect the University's property, equipment and valuables, and to facilitate the detection of any infringements.

(3) Data processing activities may not be aimed at the systematic surveillance of University employees or students.

(4) The legal basis for data processing activities is the legitimate interest of the University in relation to data processing activities.

(5) Recordings made by property protection camera systems shall be stored by our University for seven days.

(6) Detailed rules on property protection camera systems, in particular on access control and data transfer, shall be laid down in a separate chancellor's order, taking into account the provisions of this regulation.

Article 33. Additional data processing for the operation of the University

(1) The University processes data for the purpose of its proper operation, in particular in connection with document management, financial management and application processes, the organization of events and the operation of IT systems.

(2) The organizational units performing data processing related to document management are independent organizational units defined by the organizational and operational rules. The organizational unit performing data processing related to financial management processes is the Financial Directorate of the Chancellor’s Office. The organizational units responsible for data processing related to application processes are, depending on the nature of the application, the faculties or the Science Organization and Application Department of the Rector's Office, in accordance with the Organizational and Operational Rules. During the implementation and coordination of international mobility applications, personal data is processed by the International Department of the Rector's Office. The organizational units responsible for processing data related to the organization of events are the faculties and the Public Relations and Communications Directorate of the Rector's Office. The organizational unit responsible for data processing related to the operation of IT systems is the IT and Data Asset Management Department of the Chancellor’s Office. Personal data may be transferred from the organizational unit responsible for data processing to other organizational units in accordance with the provisions of Section 11 of the Regulations.

(3) The detailed circumstances of data processing related to the operation of the University, including the organizational units responsible for each type of data processing, are set out in the relevant

regulations of the University, as well as in the applicable laws governing the specific data processing and in the data processing information notices prepared on the basis thereof.

Section 34. Final provisions

This regulation shall enter into force on the day following its adoption. Upon entry into force of this regulation, all previous regulations on data processing shall cease to be effective.