BUDAPESTI CORVINUS EGYETEM	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**13/2023** Version number: **00**
ON THE RULES FOR DATA PROCESSING		

Person responsible for professional aspects:	**Barbara Bíró**	Head of Legal Affairs
Professional aspects checked by:	**Balázs Locsmándi**	Data Protection Officer
Legal aspects checked by:	**Barbara Bíró**	Head of Legal Affairs
Decision-making body:	**Presidential Committee**	
Person responsible for editing and publishing the text:	**Anikó Erős**	Higher Education Expert

Version number	Date of publication	Effective date	Version tracking
00	13.06.2023	01.08.2023	**Publication** Resolution No. ET-68/2023 (27 April)

BUDAPESTI CORVINUS EGYETEM	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**13/2023** Version number: **00**
ON THE RULES FOR DATA PROCESSING		

Table of Contents

BUDAPESTI CORVINUS EGYETEM	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**13/2023** Version number: **00**
ON THE RULES FOR DATA PROCESSING		

Objective and scope of the Provisions

1. §

(1) Pursuant to 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 referred to as the General Data Protection Regulation or GDPR), the purpose of the Provisions is to ensure that Corvinus University of Budapest (hereinafter referred to as the University), as a legal entity that is a data controller, fully complies with the GDPR and all other sectoral data protection regulations in its operations.

(2) The scope of the Provisions covers all data processing carried out by the University at its registered seat and all its business premises.

(3) The personal scope of the Provisions covers all organisational units of the University, all employees of the University, and all persons working for the University under other employment relationships or otherwise related to the University who process personal data.

(4) The material scope of the Provisions covers all personal data processed by any organisational unit of the University, the entire range of data processing operations carried out on such personal data, irrespective of the place of their creation, processing and the form in which they are presented.

Related documents

2. §

(1) Related legislation:

a) Fundamental Law of Hungary,

b) Regulation (EU) 2016/679 of the European Parliament and of the Council (of 27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as General Data Protection Regulation or GDPR),

c) Act CXII of 2011 on informational self-determination and the freedom of information.

Definitions

3. §

(1) For the purposes of this section:

a) *personal data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (e.g.: name, place of birth, Neptun ID, disability information, the fact that a person is a student of the University, the study programme a student is enrolled in, the fact that a student is enrolled in a self-funded programme or a Corvinus Scholarship programme, the fact that a student has applied for any scholarship, has been awarded a scholarship, the exams a student has registered for or the marks he or she has received, the fact that a student has taken part in the Students' Scientific Association, his or her results in the Students' Scientific Association, the fact that disciplinary proceedings have been initiated against a student or the results of such proceedings, the fact that a student has registered for a particular exam; employees' names, addresses, their mothers' names, their job titles, how long they have been working at the University, their salary and other benefits, the fact that employees hold any position or committee membership, the fact that employees have filed a complaint against a performance assessment, the fact that employees have received any remuneration, awards or honours, or have been subject to any labour law measures);

b) *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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,

c) *controller* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In these Provisions, the University is the legal entity that is the data controller, however, in this context, any organisational unit within the meaning of the Organisational and Operational Procedures that processes personal data and that determines the purposes for which personal data are processed, the scope of the data processed and the means of processing (hereinafter referred to as Data Controller) is also considered a controller. Examples of data controllers are Student Services, HR, Finance, CIAS, the Library, but also institutes and research institutes can be data controllers,

d) *processor* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, for example, an external IT operator and/or development company that may access personal data stored in the system in the course of its contractual tasks, but may not do anything with them without the consent or instruction of the data controller,

e) *personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed,

f) *restriction of processing* means the marking of stored personal data with the aim of limiting their processing in the future,

g) *profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements,

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

i) *filing system* means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis,

j) *recipient* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing,

k) *third party* means a natural or legal person, public authority, agency or body other than the data subject, data controller, processor and persons who, under the direct authority of the data controller or processor, are authorised to process personal data, e.g. the Maintainer, sectoral ministry, University consultants, IT systems companies,

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

m) *genetic data* means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question,

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

o) *data concerning health* means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status,

p) *Data Protection Officer* means the person appointed by CORVINUS to facilitate compliance with the GDPR and the exercise of data subjects' rights of control, acting in accordance with Articles 37–39 of the GDPR,

q) *data erasure* means the physical destruction or pseudonymisation of personal data,

r) *data protection contact person* means an employee designated by the manager responsible for data processing or a natural person who works for the University in another employment relationship and who is in contact with the University, the Data Protection Officer and/or the Head of Legal, Administrative and Regulatory Services (hereinafter referred to as Head of Legal Affairs) on matters relating to data protection and/or represents the organisational unit carrying out the data processing in relation to such matters.

Principles

4. §

(1) The procedures of all organisational units of the Data Controller shall comply with the principles of data processing in the exercise of data subjects' rights, in particular:

a) *Legality, fairness and transparency:* The processing of personal data shall be lawful, fair and transparent for the data subject. The principle of transparency means predictability and control over the data subject's data. This principle guarantees that the data subject is aware of how and in what form his or her data are processed.

b) *Accuracy:* Personal data shall be accurate and, where necessary, up to date; all reasonable measures shall be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay.

c) *Accountability:* The principle of accountability means, for one thing, the obligation for the Data Controller to establish the internal rules, processes and mechanisms necessary to comply with the obligations under the General Data Protection Regulation and, for another thing, the ability to demonstrate compliance.

d) *Data protection by design:* In the interests of the data subject's exercising his or her rights, the Data Controller shall take into account the state of science and technology, the costs of implementation and the nature, scope, circumstances and purposes of the processing. To implement the principle of data protection by design, it is necessary for the Data Controller to consider, identify and analyse the risks to the rights of natural persons. On the basis of the above, it can be determined how the given data

processing within the given organisation can be designed to meet the requirements of data protection by design under the circumstances identified.

I. THE UNIVERSITY'S DATA PROTECTION SETUP

Data protection roles and responsibilities

5. §

(1) General employee responsibility: The legal responsibility for data protection compliance rests with all employees of the University, including executives and other persons working for the University in another form of employment. This applies to all obligations under the GDPR and national data protection laws, and in particular:

a) compliance with data protection principles such as purpose limitation, data minimisation and lawfulness (Article 5 of the GDPR),

b) erasure or anonymisation of personal data (Articles 5, 6 and 17 of the GDPR),

c) taking appropriate technical and organisational measures (Article 32 of the GDPR).

(2) Senior executive responsibility: The Presidential Committee is committed to full compliance with the GDPR.
The President is responsible for ensuring that the University's operations comply in all respects with the requirements of the GDPR and national data protection legislation. In this context, it shall provide the material and human resources necessary for compliance, present these Provisions and verify at regular intervals, as it may determine, that operations are in line with this Provisions.

(3) Executive responsibility: In addition to the above, the heads of each organisational unit are responsible for contributing to

a) the exercise of data subjects' rights (Article 15 of the GDPR),

b) the conclusion of data processing contracts (Article 28(3) of the GDPR),

c) the compilation and updating of the data processing register under the responsibility of the Head of Legal Affairs (Article 30 of the GDPR).

(4) Executives (hereinafter referred to as executives), as specified in the Organisational and Operational Procedures, also have supervisory and organisational responsibilities (executive responsibility). All executives are responsible for ensuring that data processing in their area of responsibility complies with data protection legislation. It is up to executives themselves to determine how they perform the tasks within their scopes of duties, in strict compliance with data processing and organisational framework conditions. Appropriate organisational measures include issuing work instructions, supervising GDPR-compliant data processing, assessing the need for support measures (e.g. employee training and online tests), designing processes for the introduction of new data processing procedures, defining technical and organisational data protection

measures and taking measures including disciplinary sanctions and other labour law measures. In determining whether an executive action under this subsection is appropriate, executives may seek the assistance of the Head of Legal Affairs and the University's Data Protection Officer.

(5) The responsibilities of executives therefore include in particular:

a) keeping up-to-date records of the data processing operations carried out in the areas under their management and/or control, covering at least the data set out in Annex 1 to these Provisions,

b) reporting personal data breaches detected in the areas under their management and/or control, in accordance with these Provisions,

c) keeping records of the data protection measures taken by the organisational unit under their management and/or control, either by their own decision or at the initiative of another organisational unit or executive (e.g. HR, Corporate and Institutional Relations, Student Services, President, Rector, Chancellor) (in particular, informing employees about the processing of their personal data, requesting their consent to the processing of their personal data where appropriate, issuing internal data protection regulations) in accordance with these Provisions,

d) preparing the data protection impact assessment in accordance with these Provisions,

e) preparing for the introduction of new data processing operations,

f) preparing the conclusion of data processing contracts with external data processors engaged by the organisational unit under their management and/or control, on the basis of the guidance of the responsible legal area (Economic Law, Procurement, Labour Law Services or Legal, Administrative and Regulatory Services) and with the assistance of the Head of Legal Affairs,

g) defining and applying data security rules agreed with the Head of Information Technology and the Head of Legal Affairs,

h) assisting in the implementation of measures proposed by the Data Protection Officer and/or the Head of Legal Affairs for GDPR compliance,

i) keeping records of the external data processors engaged by the organisational unit under their management and/or control, with at least the content set out in Annex 2 to these Provisions,

j) channelling the technical and organisational measures (TOMs) for data security defined by Information Technology to the external data processor involved in the operations of the organisational unit under their management and/or control;

k) enforcing data subjects' rights under the GDPR (information, rectification, objection, data portability, erasure, restriction of processing, access to personal data) as directed by the Head of Legal Affairs (see Sections 16. §-25. § of these Provisions),

l) preparing the necessary data processing notice for the data processing operations in the areas under their management and/or control, in accordance with the guidance of the Head of Legal Affairs, notifying the Head of Legal Affairs of any change in the data processing operations in the area under their management and/or control, in order to enable the Head of Legal Affairs to fulfil the record-keeping obligations under these Provisions,

m) erasing data the data processing of which has expired,

n) investigating requests and/or implementing resolutions of the Hungarian National Authority for Data Protection and Freedom of Information in the area under their management and/or control, as directed by the Head of Legal Affairs,

o) supporting external or internal data protection audits,

p) supporting the work of the Data Protection Officer, e.g. by providing information, training or supporting data protection audits,

q) designating a data protection contact person in the organisational unit under their management and/or control,

r) developing and updating an IT authorisation profile appropriate (purpose-limited) to the job title of the employees working in the area under their management and/or control, respecting the principle of minimum authorisation.

(6) Data protection contact persons shall contribute to the implementation of the compliance measures detailed in these Provisions, as directed by the head of the organisational unit responsible for data controlling. They are responsible for keeping contact with the Head of Legal Affairs and/or the Data Protection Officer in professional matters, channelling the data protection requirements affecting their organisational unit and helping to establish GDPR compliance for which executives are responsible.

(7) The rules on the responsibility of the Data Protection Officer and his or her duties are laid down in Section 41. § of these Provisions.

(8) Specific responsibility of the Head of Legal Affairs: the Head of Legal Affairs is responsible for taking the legal position necessary for prudent data protection at the University in the event of a request and/or a shortcoming. However, the Head of Legal Affairs is not responsible for the University's GDPR compliance, which is the responsibility of the head of the relevant organisational unit; while at University level, GDPR compliance is the responsibility of the President. In the event of a data protection issue, the Head of Legal Affairs may turn to the Data Protection Officer, it being understood that the Head of Legal Affairs is not bound by the opinion of the Data Protection Officer in the formation of his or her legal opinion.

(9) The Head of Legal Affairs is responsible for keeping and updating records of all data processing carried out by the University in accordance with Article 30 of the GDPR. The Head of Legal Affairs is not responsible for updating data processing records if the

executive responsible for data processing does not give the Head of Legal Affairs sufficient information about the data processing or changes that have taken place in the area under his or her management and/or control.

(10) The Head of Legal Affairs is responsible for the legal compliance of the exercise of data subject rights and the data processing notice concerning the data processing carried out by each area, in accordance with Sections 23. § to 26. § of these Provisions.

(11) The Head of Legal Affairs is responsible for establishing data protection rules that comply with the law at all times.

(12) The Head of Legal Affairs is responsible for the preparation of data protection training material and initiates and/or contributes to the organisation of regular training for the organisational units of the University that process data.

(13) The designated specialists of Information Technology have all the authorisations necessary for the administration of IT systems and services. These are very high level authorisations allowing access to all employee-generated data. This includes correspondence, files created, internet traffic, etc. No one at the University other than the employees of Information Technology may have such authorisations, which shall be accepted by all employees of the University, including executives. Furthermore, all employees of the University shall accept the above, namely that Information Technology employees with sufficiently high authorisations are aware of all operations carried out in all IT systems and have information on all data generated.

(14) A significant part of the processing of personal data is carried out by external service providers. This includes the entire M365 service system. This is where the most part of correspondence and file processing takes place. Any changes, erasures or additions to the data stored in these systems are possible, but these data are not physically located on the University's infrastructure.

II. DATA SUBJECTS' RIGHTS AND THEIR EXERCISE

Rights enforceable by data subjects

6. §

(1) Data subjects may request information about the processing of their personal data, request the rectification and/or erasure of their personal data, except for mandatory processing, request the restriction of processing, withdraw their consent to processing, and exercise their right to data portability and their right to object as indicated at the time of collection, in accordance with Chapter III of these Provisions.

(2) The exercise of rights in these Provisions is free of charge, except where expressly indicated by the University.

Right of information

7. §

(1) The head of each Data Controller (the organisational unit of the University that processes personal data) shall take appropriate measures to ensure that all information referred to in Articles 13 and 14 of the GDPR and each communication pursuant to Articles 15 to 22 and 34 of the GDPR concerning the processing of personal data is provided to data subjects in a concise, transparent, understandable and easily accessible form, in a clear and plain language.

(2) If the Data Controller (the organisational unit of the University that processes personal data) collects personal data relating to the data subject from the data subject, it shall provide the data subject with all the following information at the time of obtaining the personal data:

a) the identity and contact details of the Data Controller (the organisational unit of the University that processes personal data) and its representative,

b) - contact details of the Data Protection Officer,

c) the purposes for which the personal data are intended to be processed and the legal basis for the processing,

d) where the legal basis for the processing is a legitimate interest, the legitimate interests of the University or a third party,

e) the recipients and/or categories of recipients of the personal data, where applicable;

f) the fact, where applicable, that the Data Controller (the organisational unit of the University that processes personal data) intends to transfer the personal data to a third country or an international organisation and the safeguards applied to such transfers,

g) the duration for which the personal data are stored or, where this is not possible, the criteria for determining that duration,

h) information on the data subject's right to request the Data Controller (the organisational unit of the University that processes personal data) to access, rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data, as well as on the data subject's right to data portability,

i) if the Data Controller (the organisational unit of the University that processes personal data) processes specific data about the data subject on the basis of the data subject's consent, information on the right to withdraw consent at any time,

j) information on the right to lodge a complaint with a supervisory authority,

k) information as to whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for the conclusion of a contract, whether the

data subject is obliged to provide the personal data, and the possible consequences of not providing the data,

l) where relevant, information on automated decision-making, including profiling, and, at least in these cases, clear information on the logic used and the significance of such processing and its likely consequences for the data subject,

m) where the source of the data is not the data subject, information about the source of the personal data and, where applicable, whether the data originate from publicly available sources.

Right of access of the data subject

8. §

(1) The data subject has the right to receive feedback from the Data Controller (the organisational unit of the University that processes personal data) as to whether his or her personal data are being processed and, if such processing is ongoing, the right to access the personal data and the following information:

a) the purposes of the data processing,

b) the categories of personal data concerned,

c) the recipients or categories of recipients to whom and/or with whom the personal data have been or will be disclosed, including in particular recipients in third countries and/or international organisations,

d) the intended period of storage of the personal data,

e) the right to rectification, erasure or restriction of processing and the right to object,

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

g) information on data sources,

h) the fact of automated decision-making, including profiling, as well as the logic used and clear information on the significance of such processing and its likely consequences for the data subject,

i) in the event of a transfer of personal data to a third country or an international organisation, the data subject has the right to be informed of the appropriate safeguards for the transfer.

(2) At the request of the data subject, the relevant organisational unit of the University shall provide the information in electronic form. If the data subject has submitted the request by electronic means, the information shall be provided in a commonly used electronic format (e.g. html, txt, pdf, jpg), unless the data subject requests otherwise.

(3) The Data Controller (the organisational unit of the University that processes personal data) shall provide the data subject with a copy of the personal data processed upon a

verified request from the data subject. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee, based on its administrative costs, as follows:

a) colour A/4: HUF 150, A/3: HUF 300,

b) black and white A/4: HUF 50, A/3: HUF 100,

c) postage according to the current postal rates,

d) labour costs for the compilation of reports and copies: HUF 3,000/hour gross (rounded to the nearest hour).

(4) The Data Controller (the organisational unit of the University that processes personal data) shall inform the data subject in advance of the above costs of providing the copy when he or she requests a copy. The right to request a copy shall not adversely affect the rights and freedoms of others, so the copy shall not contain information about another person. The rules under this subsection do not apply to the release of copies of camera recordings made by the University, given that these rules are set out in the internal rules governing the operation of the camera system.

Right of rectification

9. §

(1) The data subject may request the rectification of inaccurate personal data relating to him or her and processed by the Data Controller (the organisational unit of the University that processes personal data) and the completion of incomplete data. The data subject also has the right to rectification in respect of inaccurately recorded data or data that have changed during the processing.

(2) The new data affected by the rectification can be verified by the data subject by presenting the identity document, deed or document certifying it, and the Data Controller (the organisational unit of the University that processes personal data) records it by taking notes of it. As long as the new data is not accurately verified, the data processing shall be restricted in accordance with Section 11. § of these Provisions. There is no need to verify any data that has been changed and/or requested to be rectified, if the original provision of the data was not subject to verification of the authenticity of the data.

(3) The previous data affected by the rectification is permanently overwritten by the new and rectified data.

(4) Rectification and overwriting of previous data does not cover data for which this is practically meaningless or impracticable (e.g.: recordings recorded by electronic surveillance and recording systems and audio recordings). For these data, rectification may only cover incorrectly recorded circumstances of processing (e.g. wrong date or time).

(5) The right of rectification is not the same as the obligation of the data subject (employees, students and other data subjects) to notify the University of any change in their data within the time limits set out in the relevant internal regulations.

Right to erasure

10. §

(1) If any of the following grounds apply, the data subject has the right to obtain, at his or her request, the erasure of personal data relating to him or her by the Data Controller (the organisational unit of the University that processes personal data) without undue delay:

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 the processing,

c) the data subject objects to the processing 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,

f) the personal data have been collected in relation to the offer of information society services.

(2) If one of the above grounds applies, the data indicated by the data subject shall be erased from all databases managed by the University. In order to comply with the above obligation, the Data Controller (the organisational unit of the University that processes personal data) shall notify the data protection contact persons of the erasure of the data. If the erasure of the data is possible centrally using an IT solution, the IT area shall also be notified.

(3) The erasure of data cannot be initiated if processing is necessary

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

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or

c) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,

d) for reasons of public interest in the area of public health, or

e) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and, finally,

f) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

11. §

(1) At the request of the data subject, the Data Controller (the organisational unit of the University that processes personal data) shall restrict the processing if one of the following conditions is met:

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

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

c) the Data Controller no longer needs the personal data for the purposes of data processing, but the data subject requires them for the establishment, exercise or defence of legal claims, or

d) the data subject has objected to the data processing; in this case, the restriction shall apply for the period until it is determined whether the legitimate grounds of the Data Controller prevail over the legitimate grounds of the data subject.

(2) Restriction of processing of personal data is the marking of stored personal data for the purpose of restricting their future processing. Restriction can be done by temporarily transferring the personal data in question to another data processing system, by removing their availability to users, by temporarily erasing them from the live database, or by isolating them. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed.

(3) If the processing is restricted, personal data, except for storage, may only be processed with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person and/or for important public interests of the Union or of a Member State.

(4) The Data Controller (the organisational unit of the University that processes personal data) shall inform the data subject in advance of the lifting of the restriction on processing.

Right to data portability

12. §

(1) The data subject shall have the right to obtain the personal data concerning him or her which he or she has provided to the Data Controller (the organisational unit of the University that processes personal data) in a structured, commonly used, computer-readable format and to transmit such data to another controller and/or to request the direct transfer of the personal data to another controller designated by him or her.

(2) According to Directive 2013/37/EU, a document is a computer-readable document if it is in a file format that allows software applications to easily identify, recognise and retrieve the unique data it contains.

(3) The data subject shall have the right to data portability only if he or she has given his or her consent or if the processing is based on Article 6(1)(b) of the GDPR (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract) and only if the processing is carried out by automated means. Data portability applies to the data processed, data derived therefrom and generated by the University in the course of data processing are not required to be disclosed as described above.

Right to object

13. §

(1) The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data for the purposes of enforcing the legitimate interests of the Data Controller (the organisational unit of the University that processes personal data) or of a third party.

(2) In the event of an objection, the relevant organisational unit of the university may no longer process the personal data, unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(3) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. In the event of an objection to the processing of personal data for direct marketing purposes, the Data Controller (the organisational unit of the University that processes personal data) shall no longer process the data for this purpose. On the basis of the data subject's request, the Data Controller (the organisational unit of the University that processes personal data) shall suspend data processing until the objection has been dealt with.

Automated individual decision-making in individual cases, including profiling

14. §

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

(2) The above right does not apply if the processing:

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

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

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

The right to withdraw consent to data processing

15. §

(1) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data processed on the basis of the consent of the data subject shall be erased by the organisational unit of the University that processed the data after withdrawal of the consent, unless the data processing may continue on another legal basis.

III. PROCEDURAL RULES ON THE EXERCISE OF RIGHTS OF DATA SUBJECTS

Data subjects and their opportunities to request data protection

Identification of the request

16. §

(1) If the employee or the head of the organisational unit receiving the request has doubts as to whether the data that are the subject of the request are personal data or whether the request constitutes the exercise of rights of data subjects, he or she shall contact the Head of Legal Affairs.

Fulfilment of the request

17. §

(1) The Data Controller (the organisational unit of the University that processes personal data) acting as the recipient of the request may refuse to fulfil the data subject's request for the lawful exercise of his or her rights under these Provisions only if it proves that it is not possible to identify the data subject, despite its intention to do so.

(2) At the data subject's request, his or her request to exercise his or her rights may be fulfilled orally, after verifying and identifying his or her identity.

(3) Identity is deemed to have been verified if the request to exercise rights is received from contact details (email address, address, telephone number) processed by the University. As it is not excluded that someone may write an email in someone else's name and from

someone else's email address, due care should be taken and the reply should only be sent to the known contact details, despite any specific request by the data subject.

(4) For requests made through other channels (e.g. in person, online contact form or telephone number), the data subject shall provide at least three of the following identifiers:

a) name,

b) name at birth,

c) place and date of birth,

d) mother's name.

(5) In special cases (e.g. audio or video recording), identification is not possible using the above methods. In such cases, efforts should also be made to identify the data subject, e.g. by comparing the voice, identifying the date, time, length and topic of the recording.

Direct request to the Data Protection Officer

18. §

(1) The University shall ensure that external partners, other natural persons, employees and students have a direct email address to the Data Protection Officer for direct contact as data subjects.

Time limit for action

19. §

(1) The head of the Data Controller (the organisational unit of the University that processes personal data) shall take action on complaints and requests received electronically without delay, but within three (3) working days at the latest.

Information for recipients

20. §

(1) The Data Controller (the organisational unit of the University that processes personal data) shall inform all recipients to whom the data have been disclosed of the rectification, restriction or erasure carried out in accordance with these Provisions.

(2) The information shall include the identification of the data subject and the precise indication of the data rectified, restricted or erased. Notification under this Section is not required if it is impossible or would require disproportionate effort.

Processing of the data of the request

21. §

(1) Data generated in the course of the fulfilment of requests under these Provisions shall be processed by the organisational unit fulfilling the request together with the data concerned until the deadline for their erasure and until the limitation period for any legal claim enforced in connection with the fulfilment of the request. In accordance with the principle of transparency, the head of the organisational unit concerned shall keep records of requests, measures and replies.

External requests

22. §

(1) Any data subject (applicant, candidate, partner, former student, etc.) may submit any form of request and/or complaint regarding the processing of his or her data to any of the University's organisational units processing personal data, and the University's organisational units concerned shall deal with such requests and/or complaints.

(2) The oral complaint or request of the data subject shall be recorded in a report drawn up by the head of the organisational unit or his or her deputy.

(3) On the basis of the request, the head of the organisational unit shall prepare a proposal for the planned measures and send it, together with the report, to adatvedelem@uni-corvinus.hu for approval within seven (7) working days of the date of the report. The head of the organisational unit concerned may not respond to complaints about data processing (requests that constitute the exercise of data subject rights), may not fulfil the requests and demands contained therein, and may not respond to requests without the approval of the Head of Legal Affairs.

(4) Within three (3) working days at the latest, the Head of Legal Affairs shall examine the case on the basis of the information available to him or her and, if approved, notify the head of the organisational unit concerned to start handling the complaint or request in accordance with the proposal approved by the same.

(5) If the request is received directly by the Data Protection Officer, he or she shall forward the request, together with his or her opinion, to the head of the organisational unit responsible for investigating the matter. The head of the organisational unit concerned shall act in accordance with Sections 16. § to 21. § of these Provisions.

(6) The University's organisational unit concerned by the request shall inform the data subject of the measures taken on the request without undue delay, but no later than one (1) month from the date of receipt of the request. If necessary, in view of the complexity of the request and the number of requests, this deadline may be extended by two (2) additional months in exceptional cases, at the discretion of the Head of Legal Affairs. The head of the organisational unit dealing with the case shall inform the data subject of the extension of

the deadline within one (1) month of receipt of the request, stating the reasons for the delay.

(7) If the data subject has submitted the request electronically, the requested University's organisational unit concerned shall also provide the information in electronic format, unless the data subject requests otherwise.

(8) If the data subject contacts any of the University's organisational units by telephone with a complaint and/or request regarding the processing of his or her data, the data subject shall be informed of the contact details of the Data Protection Officer.

Employee requests

23. §

(1) Employee complaints and/or requests regarding the processing of data may be made by contacting HR and/or Finance, as appropriate. Within seven (7) working days, HR and/or Finance shall contact other organisational units as necessary to fulfil the request and the Head of Legal Affairs in order to prepare a response, and they shall provide the necessary information to prepare a response and the legal opinion, if required, within three (3) working days. The time limits for dealing with the case shall be those set out in Sections 17. § to 21. § of these Provisions. After the approval of the Head of Legal Affairs, HR and/or Finance shall respond to complaints (requests that constitute the exercise of data subject's rights) and requests relating to data processing, comply with the requests contained therein or, if the legitimate conditions for doing so exist, refuse them.

Student requests

24. §

(1) Data subjects may submit a complaint and/or request regarding the processing of student data to Student Services (SS) or Corvinus Doctoral Schools (CDS), as appropriate. Within seven (7) working days, SS shall contact other organisational units as necessary to fulfil the request and the Head of Legal Affairs in order to prepare a response, and they shall provide the necessary information to prepare a response and the legal opinion, if required, within three (3) working days. The time limits for dealing with the case shall be those set out in Sections 17. § to 21. § of these Provisions. After the approval of the Head of Legal Affairs, SS shall respond to complaints (requests that constitute the exercise of data subject's rights) and requests relating to data processing, comply with the requests contained therein or, if the legitimate conditions for doing so exist, refuse them.

The University's obligation to provide information about remedies

25. §

(1) If the head of the organisational unit concerned does not act on the request of the data subject or the request is explicitly refused, the organisational unit responsible for responding shall inform the data subject without delay, but no later than one (1) month after receipt of the request, of the reasons for non-action and of the right of the data subject to lodge a complaint with the National Authority for Data Protection and Freedom of Information and to seek judicial remedy. The reply letter concerning the refusal is drafted by the Head of Legal Affairs.

IV. INFORMATION ON THE PROCESSING OF PERSONAL DATA

General information obligations

26. §

(1) In all cases where personal data are processed (whether for employees, persons in other employment relationships, external partners, students or applicants), the executive responsible for data processing shall, prior to the processing of the data, prepare a data processing notice for the data subjects, in cooperation with the Head of Legal Affairs, and make it available to them in accordance with Section 7. § of these Provisions.

(2) The data processing notice shall always cover the following:

a) the data subjects of the processing,

b) the name and contact details of the Data Protection Officer,

c) the purpose of the data processing,

d) the scope of the data processed,

e) the duration of the processing or, where this is not possible, the criteria for determining that duration,

f) the legal basis for processing,

g) where the legal basis for the processing is a legitimate interest of the University, a brief description of that legitimate interest,

h) where the legal basis for the processing is the consent of the data subject, the right to withdraw consent at any time without affecting the legality of the processing carried out on the basis of the consent before its withdrawal,

i) the identity of any data processors or other recipients,

j) if the University transfers the data to a third country, the legal instrument used,

k) the procedure for exercising data subjects' rights,

l) the right to apply to the National Authority for Data Protection and Freedom of Information,

m) whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for the conclusion of a contract, whether the data subject is obliged to provide the personal data, and the possible consequences of not providing the data,

(3) In all cases, the data processing notice shall be drafted by the Head of Legal Affairs, with the assistance of the Data Protection Officer and/or the Data Protection Contact Person. The data processing notice can be requested by filling in the online form provided by the Head of Legal Affairs.

(4) The data processing notice drawn up shall be made available to data subjects in such a way that it can be subsequently verified (principle of accountability). It is appropriate to send the text of the notice or a clickable link to the notice to data subjects by email, and it is also appropriate to accept registration on an online registration platform only after ticking the box next to the clickable link to the data processing notice. The executive responsible for data processing is responsible for the design of the information process used, and he or she shall seek the opinion of the Head of Legal Affairs in case of doubt. The organisational unit responsible for data processing shall store the information that data processing information has been provided (data relating to the subsequent verifiability of accessibility) for a period of five (5) years or until the expiry of any legal claim that may be asserted in connection with the information, in accordance with paragraph (a) of subsection 5. §(5) of these Provisions.

Specific information obligations

27. §

(1) For data processing concerning all applicants, the data processing shall be recorded in the Data Processing Notice for Admission (DPNA). Data processing shall be deemed to concern all applicants if it concerns all applicants for the given type of programme (e.g. Bachelor programmes, Master programmes, Doctoral programmes, mobility). The availability and acknowledgement of the DPNA shall be declared by the applicants during the application process, either on paper or online, depending on the application channel (FELVI, DreamApply, Mobility, etc.). This information shall be provided by the organisational unit responsible for receiving and processing applications through the relevant application channel. In connection with the development of the information process, the Head of Legal Affairs shall, if requested, assist the executive responsible for data processing with a position paper. The Head of Legal Affairs is responsible for the content and updating of the DPNA, it being understood that the organisational unit responsible for receiving and processing applications is responsible for notifying the Head of Legal Affairs of any change in data processing.

(2) If the data processing concerns all students, it shall be recorded in the Student Data Processing Notice (SDPN). Students are informed of the data processing under the SDPN by means of their enrolment forms and/or the conclusion of their training contracts, in which a specific point in the training contract refers to the availability of the SDPN and the contract stipulates that the student acknowledges the provisions of the SDPN by signing it. The Head of Legal Affairs is responsible for the content and updating of the SDPN, it being understood that the organisational unit responsible for the academic records of students is responsible for notifying the Head of Legal Affairs of any change in data processing.

(3) If the data processing concerns all employees, it must be recorded in the Employee Data Processing Notice (EDPN). Employees are informed about data processing under the EDPN in the context of concluding their employment contracts, in which a specific paragraphrefers to the availability of the EDPN, and the employment contract stipulates that the employee acknowledges the provisions of the EDPN by signing it. The Head of Legal Affairs is responsible for the content and updating of the EDPN, it being understood that the HR department/organisational unit responsible for employee management is responsible for communicating any change in data processing to the Head of Legal Affairs.

(4) In all other cases, the executive responsible for data processing is responsible for the preparation of the necessary data processing notice for processing in the area under his or her management and/or control, under the direction of the Head of Legal Affairs, in accordance with Section 26. § of these Provisions.

V. RULES ON THE ERASURE OF PERSONAL DATA

Data erasure

28. §

(1) In the context of their data processing, organisational units of the University that process personal data shall ensure the erasure of personal data when the retention period defined for the processing has expired.

(2) Each Data Controller (organisational unit of the University that processes personal data) shall record, with the content set out in Annex 3 to these Provisions, when the data shall be erased for the different data processing operations carried out by the given area. The deadlines for data erasure are those set out in the Student and Employee Data Processing Notices. In the case of other processing, the Data Processing Notice applicable to that processing shall apply. When in doubt, the Head of Legal Affairs should be consulted. All executives responsible for data processing shall prepare an erasure process description in accordance with Annex 3 to these Provisions within one hundred and eighty (180) days of the issuance of this Instruction.

(3) The head of each area is responsible for keeping up-to-date records of the data processing activities carried out by each organisational unit, in accordance with paragraph (a) of subsection5. §(2) of these Provisions.

(4) The head of the organisational unit concerned is responsible for the erasure of data for which the data processing deadline has expired and shall rely on the data protection contact persons to carry out this task. If it is possible to erase the data by IT means, the executive shall consult with the Head of Information Technology on the solution. Automatic data erasure should be pursued within the available IT and cost constraints. The Head of Legal Affairs should be involved, where possible, in the development of the procedure for the erasure of data.

(5) The head of the organisational unit processing personal data is responsible for operating an effective erasure mechanism in accordance with the erasure process description in his or her area of management. The executive shall update any changes in the erasure process within thirty (30) days. The Head of Legal Affairs shall assist the executive in the performance of his or her duties in accordance with this paragraph at his or her request.

(6) If an external contractor (data processor) is involved in the erasure of the data, the head of the organisational unit processing personal data shall conclude a data processing contract with the data processors involved in the data erasure operations, which contract shall contain the erasure deadlines for each data processing operation, in accordance with Article 28 of the GDPR. At the request of the executive, the Head of Legal Affairs shall draw up a draft data processing contract.

VI. PERSONAL DATA BREACHES

Handling of personal data breaches

29. §

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

(2) Breaches may cause physical, financial or non-financial damage to natural persons, including:

a) the loss of control over their personal data or the restriction of their rights,

b) discrimination,

c) identity theft or similar abuse,

d) financial loss,

e) the unauthorised association of pseudonymous data with an unauthorised person,

f) damage to reputation,

g) breach of confidentiality of personal data protected by professional secrecy,

h) or other significant economic or social disadvantage.

(3) Breaches can be grouped by their nature as follows:

Destruction of data	Personal data • no longer exist, or • no longer exist in their former and usable form.
Data loss	Personal data still exist, • but the data subject is no longer able to access them, or • the data have been removed from the data subject's possession. Examples: • loss/theft of a storage device (USB stick, laptop, etc.), or • a single copy of the data is encrypted, or • the key to the encrypted data gets lost.
Data modification	Personal data • content gets changed, or • the data are incomplete, or • the data are unreadable.
Disclosure of data	The data • are received by persons who are not authorised to receive them, or • the data may be accessed by persons who are not authorised to do so. Examples: • hacker attack • incorrect disclosure • loss of data media

Categorisation of personal data breaches

30. §

(1) The Data Controller (the organisational unit of the University that processes personal data) is responsible for analysing and evaluating the breaches brought to its attention in order to take further appropriate measures for incident response.

(2) Grouping of breaches according to their severity:

a) Minor breaches: unlikely to pose a risk to the rights and freedoms of natural persons.

b) Risky breach: personal data breaches involving only a minimal risk of damage, and involving even a single natural person, should also be included here.

c) Likely high-risk breach:

(ca) firstly, a disadvantage can be assessed on the basis of the nature and content of the data (e.g. financial information or specific data, location data, internet log files, browsing history, email records and itemised call logs),

(cb) secondly, the likely consequences of the breach (e.g. if it could lead to misuse of personal data, harm to physical integrity, defamation, libel or damage to good reputation),

(cc) finally, the circumstances of the breach may also be relevant (e.g. if there is a suspicion of illegal data acquisition or a breach of an information system or data under the Criminal Code, or a circumvention of technical measures to protect the information system, or a criminal offence).

(3) The criteria for the classification of personal data breaches are set out in Annex 4 to these Provisions.

Examples of a personal data breach

31. §

(1) Employees or other persons responsible for the processing of personal data may detect personal data breaches, i.e. unlawful processing of personal data, in particular unauthorised access, alteration, transfer, disclosure, erasure or destruction, accidental destruction or accidental damage, in particular, but not exclusively, in the following places and activities:

a) unintentional (or intentionally improper) unauthorised making of recordings using electronic surveillance and recording systems, and/or unintentional storage of such recordings beyond the time limit, and/or making them available to unauthorised persons,

b) unintentional taking of photographs, and/or unintentional (or intentionally improper) storage of such photographs beyond the time limit, and/or making them available to unauthorised persons,

c) recording more data than the data controller intended when recruiting for a job advertisement, or unintentional storage of applicants' data beyond the time limit,

d) in the event of unsubscribing from newsletters at the request of the data subject, the data are not effectively and immediately erased,

e) a ransomware attack encrypts the University's databases (e.g. student databases related to newsletter distribution),

f) databases containing personal data and getting out of the control of the University. (Employees obtain data from their work equipment without authorisation, make them available to unauthorised persons or remove their work equipment containing personal data from their place of work without authorisation),

g) a cyber attack threatens the databases managed by the University (e.g. a hacker's website displays a part of a registration database),

h) documents and other data carriers that have been improperly stored or discarded after the expiry of the data processing time limit,

i) mail or email sent to the wrong recipient, or copying unauthorised recipients sending email,

j) malfunctions of data carriers (laptops, tablets, mobile phones) that compromise the security and integrity of personal data and/or theft or loss of such data carriers,

k) unauthorised access to personal data due to incorrectly configured authorisation management,

l) unauthorised access after termination of employment,

m) other malicious external attacks,

n) providing data for phishing emails.

Roles and responsibilities within the organisation

32. §

(1) Employees or persons working for the University in the context of other non-employment relationships who detect a personal data breach, i.e. unlawful processing of personal data, in particular unauthorised access, alteration, transfer, disclosure, erasure or destruction, accidental destruction or damage, in connection with personal data processed or managed by any organisational unit of the University, shall report it through their direct supervisor immediately after detection to the Head of Legal Affairs with the information set out in Annex 5 of these Provisions. The whistleblower may also provide additional information that he or she deems relevant to the identification and investigation of the breach.

(2) Detection is when an employee has reasonable certainty that a security incident has occurred that could lead to unlawful interference with personal data. The head of the organisational unit affected by the breach shall initiate an immediate investigation to determine whether a personal data breach has occurred and, if so, what action is required.

(3) The University shall set up a dedicated email address for reporting personal data breaches and ensure that it is available 24 hours a day. Email address to report personal data breaches: adatvedelem@uni-corvinus.hu

Measures outside the organisation

33. §

(1) Each Data Controller (organisational unit of the University that processes personal data), if it uses the services of an external data processor, shall conclude a data processing contract with the data processor it engages, which shall ensure that the data processor will deal with the personal data breach it detects in accordance with the provisions of these Provisions.

Measures at organisational level

34. §

(1) The Head of Legal Affairs shall act on the breach reports received by him or her, assess the level of data protection risk posed by the breach, decide whether the breach should be notified to the National Authority for Data Protection and Freedom of Information (the criteria for assessment are set out in Annex 6 to these Provisions), and decide whether the breach should be notified to the data subject(s).

(2) If the Head of Legal Affairs, in the light of the circumstances of the breach, decides that it is not necessary to inform the National Authority for Data Protection and Freedom of Information and/or the data subjects of the breach, he or she shall document the reasons and circumstances underlying his or her decision.

(3) The head of the organisational unit affected by the breach is responsible for documenting the personal data breach in sufficient detail in accordance with Annex 5 of these Provisions, and for taking reasonable emergency measures (e.g., remediation of the breach as soon as possible, such as disabling devices, disabling access, eliminating security gaps, restoring back-up copies, restoring the original state), with the assistance of the IT area, without affecting workflow, if possible, and for assessing the measures necessary to avoid similar cases.

(4) An employee or other person in a non-employment relationship who processes personal data at the University shall report any personal data breach detected within the scope of his or her activities to his or her direct supervisor and through him or her to the Head of Legal Affairs in accordance with Section 32. § of these Provisions.

Recording of breaches

35. §

(1) In the event of a breach of the data processed by the University, the Head of Legal Affairs shall examine the notification and, if required, request the whistleblower to provide additional data, which the notifier shall provide without delay, but no later than within two (2) working days.

(2) The information provided by the person who detected the breach shall contain the data set out in Annex 5 to these Provisions.

(3) Once the information has been provided, the Head of Legal Affairs shall carry out an investigation. If, as a result of his or her investigation, he or she finds that the data in question is indeed personal data or that the content of the notification constitutes a breach, he or she shall register the breach, regardless of its gravity.

(4) The following shall be entered in the records:

a) the scope of the personal data concerned,

b) the scope and number of data subjects affected by the personal data breach,

c) the date and time of the personal data breach,

d) the circumstances and effects of the personal data breach,

e) the measures taken to respond to the personal data breach,

f) the classification of the breach (records only/NAIH/notification of the data subject),

g) the names of the persons carrying out the classification,

h) the date and means of the NAIH/data subject notification,

i) other data specified in the legislation providing for the processing.

Subjects and content of the obligation to register and notify

36. §

(1) On the basis of the information provided, the Head of Legal Affairs shall propose the necessary measures to remedy the personal data breach to the head of the organisational unit processing the data.

(2) Any further measures to be taken on the basis of the proposal shall be decided by the head of the organisational unit processing the data.

(3) The head of the organisational unit processing the data shall inform the Head of Legal Affairs of the measures taken to respond to the personal data breach within two working days of the implementation of those measures. The Head of Legal Affairs shall keep records of personal data breaches for a period of five (5) years or until the end of the limitation period for any legal claims that may be brought in connection with the breach.

(4) Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the head of the organisational unit concerned by the breach shall, on the basis of a proposal by the Head of Legal Affairs, inform the data subject of the personal data breach without undue delay in a clear and comprehensible manner, with the following content:

a) name and contact details of the Data Protection Officer,

b) the nature and consequences of the personal data breach,

c) actions taken or planned to remedy the personal data breach.

(5) Specific messages should be used to inform data subjects of breaches and should not be sent in conjunction with other types of information, such as periodic updates, newsletters or standard messages. Examples of transparent information methods include direct messaging (e.g. email, SMS, direct message), prominent banner advertisements or notices on the website, information by post, and prominent advertisements in the printed press. A notification limited to a press release or a university blog post is not an effective way to inform individuals about a breach.

(6) Where it is necessary to notify data subjects of a personal data breach that has occurred, a solution should be chosen that is most likely to ensure that all data subjects are properly informed.

(7) In cases where notification of the data subject becomes necessary, the National Authority for Data Protection and Freedom of Information must always be notified, which the Head of Legal Affairs shall do.

(8) As a general rule, the University only has an obligation to notify the National Authority for Data Protection and Freedom of Information if the personal data breach is likely to pose a risk to the rights and freedoms of natural persons. The Head of Legal Affairs shall decide whether there is an obligation to notify the National Authority for Data Protection and Freedom of Information in relation to a given breach, and this decision shall be documented in all cases where the breach is not notified to the National Authority for Data Protection and Freedom of Information.

(9) If necessary, the Head of Legal Affairs shall notify the National Authority for Data Protection and Freedom of Information no later than seventy-two (72) hours after becoming aware of the breach. If the notification is not made within seventy-two (72) hours, the reasons justifying the delay shall be provided. However, no notification is required if the personal data breach is unlikely to pose a risk to the rights and freedoms of natural persons. Annex 6 to these Provisions provides examples of when a breach should or should not be reported to the National Authority for Data Protection and Freedom of Information. If it is not possible to provide the information required under Annex 5 to these Provisions at the same time, it may be provided in instalments at a later date without further undue delay.

(10) A “single” notification may also be made to the National Authority for Data Protection and Freedom of Information on multiple breaches, provided that the breaches involve personal data of the same nature that have been breached in the same way within a relatively short period of time. A single report can be made for several similar incidents reported within 72 hours. If there are a series of breaches involving personal data of different types that have been breached in different ways, the notification should be made in the usual way, i.e. each breach should be notified separately.

(11) If an incident is of low risk, it is not necessary to notify the data subjects if:

a) the personal data had been encrypted, making the data unintelligible to third parties,

b) the organisational unit of the University that is affected by the breach or the IT area have taken effective action that is likely to result in the high risk no longer materialising,

c) informing data subjects would be a disproportionate effort, in which case, for example, a notice could be issued by the organisational unit of the University that is affected by the breach.

Consequences of personal data breaches for employees

37. §

(1) In the event of a personal data breach, the Head of Legal Affairs, after investigating the breach, shall provide feedback on its occurrence and severity to the head of the organisational unit under the area of responsibility of which the breach occurred and/or during the work of an employee under the work control of which the breach occurred, and finally to the executive(s) who had responsibility for the occurrence of the breach. On the basis of the feedback, the executive shall investigate and determine whether any employee omission has occurred and, if necessary, take employer action against the employee, as required by the internal regulations for employment, based on the feedback from the Head of Legal Affairs.

VII. NEW DATA PROCESSING

Process for implementing the new data processing operations

Preparing new data processing operations

38. §

(1) If the opportunity or the need to implement new data processing operations arises in an organisational unit, the head of the organisational unit shall consult the Head of Legal Affairs and at the same time inform the Data Protection Officer in accordance with Annex 1 to these Provisions, including a description of the nature of the processing technology, if any, and the data security (process and IT) provisions applied.

(2) The head of the organisational unit shall prepare a written summary of the subject of the request, including any information, drafts, system specifications, concepts or notes relating to the processing of the data, relevant to the start of the new processing operation. The responsible head of the organisational unit concerned by the new data processing operation shall inform the Head of Legal Affairs at least by sending the following data and information in full:

a) the purpose of the data processing operation,

b) the legal grounds of the data processing operation,
c) the scope of data subjects,
d) a description of the data concerning the data subjects,
e) the source of the data,
f) the duration of the processing of the data,
g) the type of the data transferred, the recipient and the legal basis for the transfer, including transfers to third countries,
h) where the data are transferred to a third country, the measures taken to ensure an adequate level of data security,
i) the name and address of the data processor, the place of actual data processing, the activity of the data processor in relation to the data processing and the type of data processed,
j) the nature of the data processing technology used,
k) a description of the data security (process and IT) provisions applied,
l) whether the processing involves profiling (Y/N).

(3) Before starting the new processing operation, the head of the organisational unit concerned shall consult the Head of Legal Affairs, who shall provide his or her legal opinion on the proposed processing operation in writing in fifteen (15) days.

(4) The new processing operation may only be started after obtaining the legal position and/or, where applicable, the opinion of the Data Protection Officer. The decision to start the new data processing operation shall be taken by the head of the organisational unit, after obtaining the opinion of the Head of Legal Affairs and, where appropriate, the Data Protection Officer. If the opinion of the head of the organisational unit responsible for the decision to implement the new processing operation differs from the opinion of the Head of Legal Affairs or the Data Protection Officer, the head of the organisational unit concerned shall document and keep the reasons for the difference.

Preparing for a change in data processing

39. §

(1) Data processing operations for different purposes are considered as separate data processing operations, even if the scope of the data processed is the same.

(2) If data processing procedures are changed, it shall be examined whether the change is within the scope of the original processing operation or whether it creates a new data processing operation.

General procedural rules for the initiation of new processing operations and changes to processing

40. §

(1) The Data Protection Officer has the right to participate and comment in the planning, organisation and negotiation of any new data processing operation or changes to existing data processing operations. For the exercise of these powers, the head of the organisational unit shall ensure the participation of the Data Protection Officer by personal invitation.

(2) All electronic correspondence relating to new data processing operations or changes to existing data processing operations shall also be sent to the Data Protection Officer and the Head of Legal Affairs, unless either of them expressly requests not to be included in the list of recipients, after having been informed of the circumstances of the new processing operation or change.

(3) Before implementing new data processing operations or changes to existing data processing operations, the Data Protection Officer shall be involved in the process with the right to give an opinion on the legality, adequacy, appropriateness and efficiency of the new data processing operations.

(4) If the legal basis for the data processing is a legitimate interest within the meaning of Article 6(1)(f) of the GDPR, the Head of Legal Affairs, with the assistance of the organisational unit concerned, shall carry out the balancing of interests test and inform the Data Protection Officer thereof.

(5) Should the GDPR require it for the data processing operation, the Head of Legal Affairs shall carry out a data protection impact assessment with the assistance of the Data Protection Officer.

(6) Within fifteen (15) days prior to the implementation of the new data processing operation or, in the case of a change in an existing data processing operation, to the entry into force of the change, the Head of Legal Affairs shall change the necessary documents in relation to the new and/or changed data processing operation and shall enter the data processing operation in the University's data processing register.

VIII. RULES ON THE DATA PROTECTION OFFICER

Appointment of a Data Protection Officer

41. §

(1) The University is required to appoint a Data Protection Officer under Article 37(1)(a) of the GDPR. The Data Protection Officer shall be appointed on the basis of his or her professional competence and, in particular, his or her expert knowledge of data protection law and practice and his or her ability to perform the tasks referred to in Article 39 of the GDPR. The Data Protection Officer may be an employee of the University or may carry out

his or her duties under an engagement contract. Communication shall publish the name and contact details of the Data Protection Officer on the University's website. The National Authority for Data Protection and Freedom of Information shall be informed of the Data Protection Officer's data using the online reporting interface operated by the Authority and shall be the responsibility of the Head of Legal Affairs.

Legal status of the Data Protection Officer

42. §

(1) All organisational units of the University that process personal data shall ensure that the Data Protection Officer is involved in all matters relating to the protection of personal data in an appropriate and timely manner.

(2) All organisational units of the University that process data shall support the Data Protection Officer in the performance of his or her tasks referred to in Article 39 of the GDPR by providing him or her with the resources necessary to carry out those tasks, to have access to personal data and processing operations and to maintain the Data Protection Officer's expert level of knowledge.

(3) All executives of the University shall ensure that the Data Protection Officer does not take instructions from anyone in the performance of his or her duties. The University may not dismiss or sanction the Data Protection Officer in connection with the performance of his or her duties. The Data Protection Officer reports directly to the President.

(4) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
.

(5) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

Tasks of the Data Protection Officer

43. §

(1) The Data Protection Officer shall have at least the following tasks:

a) to provide information and professional advice to all executives of the University under the University's Organisational and Operational Procedures, as well as to employees, students and other data subjects who are data controllers, on their obligations under the GDPR and other EU or Hungarian data protection provisions,

b) to monitor compliance with the GDPR, with other EU or Member State data protection provisions and with the internal rules of the University in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits,

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance,

d) to cooperate with the supervisory authority,

e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

(3) The Data Protection Officer may fulfil other tasks and duties. The Data Controller or data processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Miscellaneous and final provisions

44. §

(1) The Technical and organisational measures ("TOM") for data security defined by IT shall be prepared by the Head of Information Technology in cooperation with the Head of Legal Affairs by 31 December 2023 at the latest.

(2) The present Provisions shall enter into force on 1 August 2023.

(3) With the entry into force of these Provisions, the Data Processing Regulations adopted by the Senate at its meeting of 14 December 2015 by Resolution No. SZ-71/2015/2016 (14 December 2015), as amended several times, shall be repealed.

Annexes:

1. Annex 1: Template for keeping records of data processing by each organisational unit
2. Annex 2: Template for keeping records of data processors
3. Annex 3: Data erasure process description template
4. Annex 4: Criteria for assessing the risk posed by a personal data breach
5. Annex 5: Breach reporting form
6. Annex 6: Examples of when to report a breach to the National Authority for Data Protection and Freedom of Information and/or when to notify data subjects

Annex 1:

Template for keeping records of data processing by each organisational unit

FORM
For keeping records of data processing operations

Name of the person who filled in this FORM:	
Name of the CORVINUS area concerned:	
Date of completion of the FORM:	

Name of the data processing[1]	Data subjects[2]	Scope of the data processed[3]	What is the purpose of the processing?[4]	Recipients of the data[5]	Description of the recipient's activities on the personal data[6]	What is the duration of data processing?[7]	Are the data transferred to a third country?[8]
1)							
2)							
3)							
4)							
5)							
6)							
7)							

[1] If the data processing does not have a name, please give it a name that best reflects the essence of the data processing. If there is already a name for the data processing (e.g. in a data processing notice), please provide that name**.**

[2] Data subjects can be e.g. employees/employees under an engagement contract/lecturers/students/visitors/alumni community members/etc. Where appropriate, more than one category may be indicated. If you need to identify additional data subjects within a category (e.g. students – exchange students, doctoral students), please indicate this circumstance when filling in the form.

[3] Specify exactly what personal data the area processes. Personal data can be anything that can be linked to an identifiable natural person.

[4] Please be as specific as possible about the purpose of the data processing. Describe as clearly as possible why the data need to be processed, what process the data are needed for, etc.

[5] Please indicate here any third parties (e.g. partner university, Educational Authority, higher education information system, external contractor, National Doctoral Council, etc.) who may receive/access the personal data you process in any capacity.

[6] Describe, to the best of your knowledge, the purpose for which the recipient receives the personal data and what the recipient will do with the personal data transferred to them.

[7] Specify how long the data should be stored/used, taking into account the requirements of the legal environment.

[8] States outside the European Economic Area (EEA) (the EEA includes EU Member States plus Iceland, Liechtenstein and Norway).

What is the legal basis for data processing?[9]	If the legal basis for the data processing is a legal obligation, which legislation creates this obligation?	Does the data processing involve any automated decision-making and/or profiling?[10]	Have Legal, Administrative and Regulatory Services been already informed of the data processing? (Y/N) If yes, then when?	If the data are transferred to a data processor, has a data processing contract been concluded with the data processor?[11]
1)				
2)				
3)				
4)				
5)				
6)				
7)				

[9] The legal basis for the data processing may be (i) the data subject's consent; (ii) a legal obligation or a public interest; (iii) a legitimate interest of CORVINUS; and (iv) the conclusion of a contract with the data subject or the performance of a contract already concluded.

[10] *profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; *automated decision making* means decision making about a data subject, without any human intervention, used in the course of data processing, which produces legal effects concerning the natural person or significantly affects him or her.

[11] If the data are transferred to a recipient, has CORVINUS entered into a data processing contract with that recipient?

Annex 2:

Template for keeping records of data processors

Name of the person who filled in this FORM:	
Name of the CORVINUS area concerned:	
Date of completion of the FORM:	

Name of the data processing operation for which the processor is used	Name of the data processor	Address of the data processor	Brief description of the data processing activity carried out by the processor
1)			
2)			
3)			
4)			

Annex 3:

Data erasure process description template

Name of CORVINUS organisational unit	Head:	Data protection contact person:

Serial number	Name of data processing*	Deadline for data erasure
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

** Fill in the data processing activities and the corresponding erasure deadlines for each organisational unit in the table.*

Processing serial number	Description of the erasure process**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	

** *Brief description of the erasure procedure applied for the data processing of the relevant serial number (e.g. "manual erasure of data until 31 January of the year following the year in question", "the IT system automatically erases the data at the parameterised time", etc.)*

Annex 4:

Criteria for assessing the risk posed by a personal data breach

Type of breach	The nature of the breach affects the level of risk. Example: If medical records (personal health data) are made available to unauthorised persons, the consequences can be more serious than the destruction of the same data.
Type and sensitivity of personal data	The more sensitive the data, the greater the risk that the breach will violate the rights of the data subject. Example: Basically, risk always depends on the context. In general, however, it can be said that the company email address (xy@Egyetem.hu) usually poses little risk to the data subject. The risk is higher with bank data, movement profiles, health data, shopping behaviour data and other sensitive data.
Easy identification of data subjects	The easier it is to identify data subjects, the higher the risk. Therefore, if the identity is already derived from the data, the risk is correspondingly high; if, however, time-consuming research is required, the risk is reduced.
The severity of the consequences for data subjects	The more serious the breach, the more negative the (potential) consequences for the data subject. Examples: identity theft, financial and non-financial damage, compensation for violation of moral rights, damage to reputation. If the data are assumed to be held by an unknown or malicious party, the risk should be set accordingly higher.
The specific situation of the data subjects	If the data subjects are particularly sensitive from a data protection point of view due to their specific situation, the risk is higher. Example: children
Number of data subjects	In general, the larger the number of data subjects, the higher the data protection risk of a breach. It should be noted, however, that depending on the nature and context of the personal data, a breach can have serious consequences for one data subject alone.

Annex 5:

Breach reporting form

The person who detected the personal data breach	
Name:	
Phone number:	
Email address:	
Organisational unit:	
The personal data breach:	
Place, date and time of detection:	
Place, date and time of occurrence:	
Description and circumstances:	
Impact:	
Scope of the data concerned:	
Number and scope of data subjects:	
Measures taken for elimination:	
Measures taken to prevent, eliminate and reduce the damage:	

Annex 6:

Examples of when to report a breach to the National Authority for Data Protection and Freedom of Information and/or when to notify data subjects

Description of the breach	Notification of the NAIH	Notification of the data subject
Loss of a properly encrypted and archived database	No	No
A ransomware virus is encrypting your database. The investigation showed that the virus only encrypted the data and did not send it on.	Yes	No
A data processor detects a bug in the website code that could be exploited to access another user's data.	Yes	Yes
Forwarding a document containing personal data to the wrong address due to a clerical error.	Yes	Yes
An unplanned power outage is causing the Data Controller's records of its customers to be unavailable for a short period of time.	No	No
A cyber attack results in the online publication of usernames and passwords.	Yes	Yes
When sending a direct marketing email, each recipient can find out the email addresses of additional recipients by using the additional recipients or copy field.	Yes	Yes

Guidance WP250rev.01 of Working Group 29 on personal data breach notification under Regulation (EU) 2016/679 sets out the cases in which a personal data breach is likely to pose a low risk to individuals' rights.

The Working Group has explained that even a breach of confidentiality of personal data encrypted with state-of-the-art algorithms constitutes a personal data breach and should be reported. If, however, the

confidentiality of the key is intact (i.e. the key has not been compromised by any breach of security and has been generated in such a way that it cannot be discovered by any available technological means by anyone who is not entitled to access the key), then the data are in principle unintelligible. The Working Group also stressed that even if the data are encrypted and the confidentiality of the key is intact, but the data controller does not have adequate back-up copies of the data, there is still a risk of data loss.

Consequently, where personal data have been rendered essentially unintelligible to unauthorised parties and a copy or back-up copy still exists, a breach of confidentiality of properly encrypted personal data need not necessarily be reported to the supervisory authority. At the same time, it should be borne in mind that a notification may not be necessary initially if there is unlikely to be a risk to the rights of data subjects; this may, however, change over time and the risk may need to be reassessed. For example, if the key is subsequently found to have been compromised or a vulnerability is discovered in the encryption software, a notification may be required.