Data Protection Regulation
of the University of Pécs

2018 Pécs

Effective from 25th May 2018

Pursuant to Act CCIV. of 2011. on National Higher Education (hereinafter HEA), Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter Privacy Act), Act XLVII of 1997 on the processing and protection of health data (hereinafter Health Privacy Act), 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 GDPR), the Senate of the University of Pécs (hereinafter University) has adopted the following Data Protection Regulation (hereinafter Regulation).

CHAPTER I.
THE PURPOSE AND SCOPE OF THE REGULATION

Article 1. (1) The purpose of this Regulation is to define the legal order of the processing of personal data by the University as a data controller, furthermore to ensure that the requirements set by the constitutional principles of data protection, the right of informational self-determination, and security of data are fulfilled.

(2) The material scope of this Regulation shall cover all personal data processing by any organizational unit of the University. The special provisions pertaining to personal data concerning health are set out in the Health Data Protection Regulation of the University. In relation with personal data concerning health, this regulation shall apply with the derogations set out in the Health Data Protection Regulation.

(3) The personal scope of this regulation shall extend to persons having civil servant status, other employment-related status or student status at the University, and to any natural or legal person affected by the data processing of the University.

CHAPTER II.
DEFINITIONS AND PRINCIPLES

Article 2. For the purpose of this Regulation

a) personal data: any information relating to an identified or identifiable natural person (‘data subject’), who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

b) sensitive data: any data included in the special categories of personal data, namely the personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, genetic data, biometric, personal data concerning health, and personal data concerning sex life or sexual orientation;

c) personal data concerning health: any data concerning the physical, mental, psychological health, pathological addiction, circumstances of an illness or death, the reason of death, disclosed by the data subject or by others in relation to the data subject. Data perceived, examined, measured, mapped or derived by a health institution. Furthermore, any data that influences and can be connected to the foregoing (e.g. behavior, environment, occupation);

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

e) data process: the set of data processing operations carried out by the processor acting on the basis of the commission or order of the controller.

Article 3. (1) The University shall undertake its data processing activities pursuant to the principles set out in Article 5. (1) of GDPR, which are lawfulness, fairness, and transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity, and confidentiality.

(2) The University, in compliance with the principle of data protection by design and by default set out in Article 25. of GDPR, shall take appropriate technical and organizational measures to ensure the compliance with the provisions pertaining to the University's data processing.

(3) Every organizational unit of the University shall ensure that the University is able to demonstrate compliance with the principles and provisions pertaining to the University's data processing (accountability).

CHAPTER III.
DATA PROCESSING AND DATA PROCESS

Article 4. (1) The University shall be the controller of any data processing carried out at the University. The University shall carry out its data processing activities through its organizational units entitled to data processing (hereinafter controller organizational unit). The records of processing activities shall contain the controller organizational unit of the certain data processing.

(2) By way of derogation to the foregoing, if the special purpose of the data processing so requires and the purpose of the data processing is defined individually by one of the University's organisational unit or the status of the controller is prescribed by law, then a given organisational unit of the University or a given institution maintained by the University may be considered a controller. This fact shall be clearly marked in the record for data processing. Where this Regulation mentions the University as the controller, the controller prescribed in this Article shall also be considered as the controller, unless it clearly follows otherwise from the text.

(3) The University may use a data processor for certain data processing activities. The data processor shall process data in the name and for the benefit of the controller based on the commission, and in particular cases according to the explicit orders of the controller. Data processor may be a third person in contractual relationship with the University or in data processing where the controller is not the University, an organizational unit of the University.

(4) If the data processor is a third person, then the terms and conditions of the data process shall be stipulated in a written agreement. The agreement may be concluded as part of a separate contract. The terms and conditions of the data process between a given organizational unit of the University or institutions maintained by the University and the controller organizational unit may be set out in University regulations or orders.

(5) The data process may be prescribed by law, in this case, the given law shall apply to legal relations of the data process. If the given law regulates the legal relation of the data process to its full extent, then entering into a written agreement is not needed.

(6) The agreement, regulation or order of the data process shall include at least the following

a) the subject, purpose and duration of the data process, the type of personal data processed, and the scope of data subjects;
b) unless otherwise provided by law, the data processor shall process the data pursuant to the written instructions of the controller. Furthermore, the situation of giving the instructions, in particular, the name of the instructing organizational unit or person;
c) whether the processor is eligible to commission further processors and if so entitled, the obligation to provide information in relation with the commission or change of the further processor;
d) the data security measures that were taken by the processor;
e) the rules on information about data breach;

f) the rules on cooperation pertaining to ensuring the data subject's rights;
g) the secrecy obligation of the processor;
h) the obligation of the processor that, unless otherwise provided by law, upon termination of the data process every personal data (including the copies) shall be either erased or returned to the controller according to the decision of the controller;
i) the processor shall provide all information that is necessary for the controller to fulfill its legal obligations;
j) the processor shall provide all information necessary for the controller to demonstrate compliance with the law and shall cooperate during the monitoring, inspection or audit of the processing by a processor.
k) the further rights and obligations of the processor and controller if needed.

CHAPTER IV.
RULES OF DATA PROCESSING
PURPOSE OF DATA PROCESSING

Article 5. (1) The University shall process personal data for purposes in relation to its operations, in particular for the purposes of higher education (instruction, scientific research, artistic activities), employment, marketing and direct marketing, operating dormitories, operating personnel and property security tools, administrative processes, IT services and information security solutions in relation to the operations of the University, utilization of the University's data properties, library, archive and language exam service, health services in accordance with the health data protection regulation of the University and other purposes set out in the Deed of Foundation of the University.

(2) The University may process data for other purposes if the requirements set out by the law are fulfilled.

(3) The exact purposes for a given data processing are listed in the record for data processing.

LEGAL GROUNDS FOR DATA PROCESSING

Article 6. (1) The university may process personal data, if

a) the data processing is ordered by statute, or by municipal decree based on statutory authorization, for executing a task in relation to the public interest or exercising public authority (compulsory data processing). These kinds of data processing are, in particular, data processing for the purposes of higher education activities, employment, public education or providing health services;
b) the data processing is necessary to fulfill a legal obligation. This kind of data processing is, in particular, data processing essential to comply with an obligation derived from a piece of legislation;
c) the data subject consented to the data processing pursuant to subsections (2)-(4) of this Article. These kinds of data processing are, in particular, data processing in relation with newsletter subscriptions, participating in sweepstakes or events, surveys or participating in scientific research;
d) the data processing is necessary to deliver a contract to which the data subject is a party or it is necessary to take steps requested by the data subject prior to the agreement. This kind of data processing is, in particular, data processing in relation to a voluntarily available service provided by the University;
e) the data processing is necessary to protect an interest which is essential for the data subject's or another person's vital interests;
f) the data processing is necessary for the controller or a third person to ensure their legitimate interests, except, if the interests or fundamental rights of the data subject that necessitate the

protection of personal data, in particular, if the data subject is a child, take precedence over these legitimate interests.

(2) Consent 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. The data subject may revoke his or her consent at any time.

(3) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing and received preliminary information (Article 7) in relation to the processing of his or her personal data. Willingness is not demonstrable if the consent was given by a specific group of subordinate data subjects collectively without exception to a data processing solely for the benefit of the University.

(4) The consent may be given in any form, where the data subject is identifiable and the fact of the consent is fixed, in particular,
a) in writing (with the signature of the data subject);

b) electronically, following the individual identification (e.g. identification via educational system), if the fact of the consent is fixed (logged);

c) electronically via the e-mail address of the data subject registered at the University if the message can be saved without modifications.

(5) Where processing is based on the balance of interests, the process of balancing and its result shall be documented. The document shall be an Annex to the record for data processing.

(6) Before processing based on the balance of interest, the controller organizational unit shall consult with the data protection officer or, in the case of data concerning health, with the health data protection officer.

(7) Sensitive data shall be processed exclusively if at least one of the conditions prescribed in Article 9 (2) of the GDPR persists.

REQUIREMENT OF PRELIMINARY INFORMATION OF THE DATA SUBJECT

Article 7. (1) If the University collects personal data from the data subject, the data subject shall be informed prior to the processing as defined in Article 13 of the GDPR, in particular, but not limited to about

a) the purpose and legal ground of the processing;
b) the estimated period of the processing or the aspects of the determination of the period;
c) the contact information of the controller and its representative and the name and contact information of the internal data protection officer of the institution;
d) the rights of the data subject and possibilities of legal remedy;
e) in particular cases, the recipient of the personal data and the categories of recipients;

(2) If the University collects the personal data from someone other than the data subject, the data subject shall be informed prior to the processing as defined in Article 14 of the GDPR, in particular, but not limited to about
a) the information listed in subsection (1) of this Article;
b) the categories of personal data processed;
c) the source of personal data and if the source of the personal data is publicly accessible.

(3) The information listed in subsections (1) and (2) shall be drawn up in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

(4) The document giving preliminary information to the data subject shall be an Annex to the record for data processing described in Article 9.

OBLIGATION OF SECRECY

Article 8. The employees taking part in data processing or data process at the University shall handle the data confidentially and secretly. The employee to be taking part in data processing or data process or the employee who has knowledge of personal data shall sign a non-disclosure statement.

THE RECORDS FOR DATA PROCESSING

Article 9. (1) As authorized by this Regulation, with the purpose to register data processing activities at the University and to define special rules pertaining to particular data processing activities, a record for data processing shall be made to every data processing. The record for data processing shall be made by the head of each controller organizational unit, with the professional help of the data protection officer, if required.

(2) The draft of the register shall be sent to the data protection officer to provide an opinion. For personal data concerning health, the draft shall be sent to the health data protection officer. The register shall be approved by the Legal Department of the Chancellor's Office with a view to the written opinion of the (health) data protection officer.

(3) The approved register shall be duly signed in witness by the head of the Legal Department of the Chancellor's Office and the head of the controlling organizational unit. One original copy of the witnessed register shall be kept by both the head of the controlling organizational unit and the (health) data protection officer.

(4) The register may be made and stored in electronic form, in this case, it shall be witnessed via electronic approval after individual identification.

(5) The data protection register shall document the basic situations of the data processing and regulate particular questions pertaining to it, within the limits of the law and University regulations. The basic situations of data processing are, in particular

a) the name and a short explanation of the data processing;
b) the name and contact details of the controller and its representative, and of the data protection officer;
c) the name of the controller organizational unit, its contact details, the name of the head of the organizational unit, the name and contact details of the data protection contact person;
d) In the case of the use of a processor, the purpose and other situations of the data process, the name of the processor, its contact details, place of the data process, and the availability of the processor agreement;
e) the indication of the legislation pertaining to the processing;
f) the purpose(s) of the processing;
g) the legal ground(s) for the processing;
h) the scope of the data subjects and their (estimated) number;
i) the scope of registered data types;
j) the source of the data (the data subject, or other processing);
k) usual data processing operations (storage, alteration, update, selection, structuration, transmission, etc.)
l) the methods of processing (manual, computerized, mixed);
m) the list and explanation of the controller's obligations (obligation of notification, impact assessment and preliminary consultation, ensuring the accuracy and actuality of data);
n) the measures that were taken in relation with data security (including the ensuring of the principles of data protection by design and by default);

o) the period of retention and time of erasure.

(6) The data protection registers shall contain the following as annexes

a) the detailed rules on the exercise of the data subjects' rights;
b) the rules pertaining to the external data transmission, in particular, the provisions concerning the recipients, the possible legal grounds, and the scope of typically transmitted data, and the detailed rules pertaining to data transmission to third countries, if necessary;
c) if the legal ground of the processing is the balance of interests [Article 6. (1) f)], the explanation of the performance and the result of the balance of interest;
d) if necessary for the given processing, the result of the impact assessment and of the consultation with the supervisory authority;
e) if necessary, additional information about the controller's obligations and the measures taken in relation with data security;
f) the text of the data processing information sheet;
g) the text of the legislation pertaining to the processing.

(7) The register shall be supervised and updated by the head of the controller organisational unit, with the help of the (health) data protection officer if needed so, as required, particularly, in cases of change in competence, other changes pertaining to the organisational unit (reorganisation), or change in the basic situations of the processing. After the termination of processing, the controller organizational unit shall put the register in the archives.

DATA PROTECTION IMPACT ASSESSMENT AND PRELIMINARY CONSULTATION WITH THE AUTHORITY

Article 10. (1) The University shall carry out an impact assessment about the possible impact of the planned processing activities on the protection of personal data, if a particular new processing possibly involves a high risk in relation to the rights and freedoms of the data subjects, with particular consideration of the application of new technologies and of the nature, scope, circumstances, and purposes of processing.

(2) Carrying-out of an impact assessment shall be mandatory in the following cases

a) systematic monitoring of a publicly accessible area on a large scale, e.g. use of an electronic surveillance system (CCTV);
b) processing on a large scale of data concerning health;
c) systematic and extensive evaluation of personal aspects relating to natural persons which are based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
d) that processing that is on the list of the kind of processing operations which are subject to the requirement for a data protection impact assessment made public by the supervisory authority.

(3) Carrying-out of an impact assessment shall not be mandatory if the processing is based on law (compulsory processing) and if the processing is necessary to fulfill a legal obligation, furthermore, if the processing is on the list of the kind of processing operations for which no impact assessment is required made public by the supervisory authority.

(4) The assessment shall contain at least

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law and University regulations taking into account the rights and legitimate interests of data subjects and other persons concerned.

(5) The impact assessment shall be carried out by the controller organizational unit. To evaluate the risks and other aspects of the assessment the controller organizational unit shall consult with the (health) data protection officer.

(6) For the processing implemented by external resources (particularly tendering), where carrying-out of the assessment is mandatory, these resources shall cover the costs of the carrying-out of the assessment. The prospective controller organizational unit or the unit responsible for the tender shall consult with the (health) data protection officer about the necessity of the assessment prior to the submission of the tender.

(7) For impact assessment concerning the students' data, the controller shall consult with the affected Student Union.

(8) The result of the assessment shall be sent to the (health) data protection officer. The (health) data protection officer may make remarks about the assessment. If the planned processing is realized, the assessment shall be attached to the register of data processing.

(9) Prior to the processing, the University shall consult with the supervisory authority in cooperation with the data protection officer, if the assessment concludes that the processing would de facto involve high risks, in the lack of measures taken to mitigate these risks. The opinion of (health) data protection officer shall be obtained about the necessity of preliminary consultation.

THE RIGHTS OF THE DATA SUBJECT

Article 11. (1) The data subject shall be entitled to exercise the rights set out in Article 15-22. of the GDPR, in particular, as follows

a) the right to access the information defined in the GDPR relating to him or her;
b) the right of rectification of the inaccurate or incorrect data relating to him or her;
c) in cases prescribed by law, the right of erasure of the data or restriction of processing;
d) the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a commonly used format and have the right to transmit those data to another controller;
e) the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on GDPR provisions pertaining to the balance of interest, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise or defense of legal claims;
f) the right to the restriction of the processing of data relating to him or her pursuant to the GDPR.

(2) The rights listed in subsection (1) shall be exercised at the request of the data subject. The request shall be submitted to the competent administrator defined in the register of data processing. If the exercise of rights results in the disclosure of personal data, then the data subject shall be identified, in particular, as follows

a) in writing (with the signature of the data subject);
b) electronically, following the individual identification (e.g. identification via educational system), if the fact of the access is fixed (logged);
c) electronically via the e-mail address of the data subject registered at the University if the message can be saved without modifications.

d) orally (personally or on phone), if the identification is ensured through the check of a personal identification document, through the personal acquaintance of the administrator and the data subject, or through the check of at least four identification information, including the login name used for the educational system, if the data subject has one.

(3) The access to personal data shall be ensured in a manner that the personal data of others shall not be disclosed for the data subject.

(4) The University may ensure the exercise of data subjects' rights via electronic means granting direct access, rectification or erasure.

(5) Detailed conditions for the exercise of data subjects' rights shall be set out in the record for data processing.

(6) Pursuant to Article 12 (1) of Act CLV of 2009 on the Protection of Classified Information, the person managing classified information may refuse to provide the information to the person concerned under the Privacy Act, if the public interest underlying classification was endangered by providing such information to the person concerned about the management of his personal data.

Article 12. In case of infringement of the data subject's rights, he or she may turn to the head of the controller organizational unit. If the data subject disagrees with the opinion of the head of the controller organizational unit, he or she may turn to the (health) data protection officer.

CHAPTER V.
DISCLOSURE OF THE DATA

Article 13. (1) The disclosure of data may happen as internal data transfer, data transfer to a third person, data transfer to a third country, public disclosure.

(2) Data transfer shall mean disclosure of data to a defined third person, including consultation and making extracts. The following shall not be regarded as data transfer: the data transmission in between the organizational units of the University as a controller, the handing-over of the data to the processor, access of the data subject to his or her own personal data.

(3) Data transfer to a third country shall mean data transfer to a country outside of the European Economic Area (EEA).

(4) Public disclosure shall mean that the data is made publicly available to anyone.

Article 14. (1) The University shall handle personal data confidentially. Data transfer, data transfer to third countries or international organizations, and public disclosure of personal data shall only happen with full compliance with the relevant rules and pursuant to Articles 16-19.

(2) The controller organizational unit shall decide about the data transfer, data transfer to third countries or international organizations, and public disclosure of personal data. In case of any doubts in relation to lawfulness, the head of the controller organisational unit is entitled (in the cases defined in Article 16. (3) and Article 18. (2) he or his is obliged) to turn to the (health) data protection officer, who shall make a resolution pertaining to the lawfulness of the planned processing operations.

INTERNAL DATA TRANSFER

Article 15. (1) Within the organizational structure of the University, the data controlled by it may be transferred to an organizational unit that needs the data to complete its tasks prescribed by the law, by the University's regulations or orders, to the extent and time of the task at hand (hereinafter: internal data transfer).

(2) If there is a dispute regarding the task at hand between the controller organizational unit and the organizational unit that seeks to receive the data, then the head of the organizational unit having competence over both units shall decide. If there is no such head, the rector or the chancellor shall decide, based on the share of competences prescribed in the HEA.

(3) The fact of the data transfer shall be put down in a report signed by both heads of the organizational units concerned if either the sending or the receiving unit requests and the transfer falls outside of the normal and regular daily tasks of the University (irregular data transfer). The irregular data transfer means especially the data transfer concerning the change in a given unit's tasks and the data transfer falling outside of the normal and regular daily tasks of the unit, which concerns at least 30 % of the data processed at that unit.

(4) When applying subsection (3), the following facts shall be put on the record

a) name of the controller organizational unit, the source of the data;
b) the name of the recipient organizational unit of the transfer;
c) the name, assignment and contact information of the administrators;
d) the purpose of the data transfer;
e) the time and date of the data transfer;
f) the scope and (estimated) number of persons concerned by the data transfer;
g) the scope of the transferred data;
h) the method of data transfer (manual, electronic, mixed);
i) the applied measures of data protection if needed.

(5) Both the sending and the receiving unit shall keep a copy of the record, a third copy shall be kept by the (health) data protection officer. The report may be made and stored electronically if authenticity is ensured by electronic approval after individual identification.

(6) It is not needed to make a report in the cases described in subsection (3), if the fact of data transfer is put down authentically (docketing) and the docketed document contains the points a)-i) of subsection (3).

DATA TRANSFER BASED ON AN EXTERNAL REQUEST

Article 16. (1) The request submitted by an individual or an external organization to transfer data within the EEA shall only be fulfilled and data shall only be transferred for other purposes if at least one of the conditions (legal grounds) set out in Article 6 (1) of this Regulation persists. The possible legal ground(s) and other situations of the transfer shall be recorded in the register for data processing.

(2) Where processing is based on consent, the consent shall explicitly cover the data transfer.

(3) Where data processing is necessary to deliver a contract to which the data subject is a party and where data is processed based on the balance of interests, data shall only be transferred on exceptional and duly justified cases after consultation with the (health) data protection officer, if the legal conditions of the transfer demonstrably persist without any doubts.

(4) No request for data transfer shall be fulfilled, if its lawfulness cannot be determined unequivocally due to the deficient or unclear content of the document (especially the consent of the data subject) based on which the data is transferred or due to other circumstances.

(5) Otherwise, Article 6 (2)-(6) shall be applied mutatis mutandis for the data transfer.

(6) The rector and chancellor of the University shall be informed about data requests from the national security services by the head of the concerned unit. The rector or the chancellor may lodge a non-suspensory complaint to the competent minister in relation to these requests.

(7) The data subject or other person or organization shall not be informed about the data request or consultation of the national security services and the measures taken, including the fact of the request or the consultation.

Article 17. (1) The circumstances of the data transfer shall be documented with at least the following content

a) the name of the controller organizational unit, the source of the data;
b) the recipient of the data transfer and the contact information;
c) the name, assignment and contact information of the administrators;
d) the purpose of the data transfer;
e) the legal ground of the data transfer;
f) the time and date of the data transfer;
g) the persons concerned by the data transfer;
h) the scope of the transferred data;
i) the method of the data transfer (manual, electronic, mixed).

(2) The requirement of documentation is fulfilled, if the fact of the data transfer and the information set out in subsection (1) are laid down authentically (docketed or logged), especially if the transfer is realised through written correspondence or pursuant to the procedure and rules prescribed in the University's regulation pertaining to the exchange of information.

(3) If the requirement for documentation cannot be solved otherwise, a report shall be made, that includes the information set out in subsection (1), except for the data transfer based on the obligation to give regular information prescribed by law.

(4) To ensure the rights of the data subjects in relation to the data transfer, a register for data transfer shall be kept, which includes the name of the data subject, the ES login name (in the lack of it, other data necessary for identification), time of the transfer, name of the recipient organisation. The (health) data protection officer shall be granted access to the register.

DATA TRANSFER TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

Article 18. (1) Data transfer to third countries or international organizations shall only happen pursuant to Chapter V of the GDPR. Article 17 shall be applied mutatis mutandis to the data transfer.

(2) The controller organizational unit shall consult with the (health) data protection officer about the persistence of legal requirements prior to the data transfer.

PUBLIC DISCLOSURE OF PERSONAL DATA

Article 19. Article 16. (1)-(5) shall be applied mutatis mutandis for the public disclosure of personal data controlled by the University.

CHAPTER VI.
DATA SECURITY

Article 20. (1) The University shall implement appropriate technical and organisational measures to ensure a level of security appropriate, including, in particular, the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a breach.

(2) The University shall implement the eventual security measures taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

(3) In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

MANUAL DATA PROCESSING

Article 21. (1) The following measures shall be implemented in relation to the security on manual (non-electronic, usually paper-based) data processing.

a) Fire and property security: The docketed documents shall be placed in a dry, locked premise suitable for storing documents.
b) Access security: Only the competent administrators shall have access to the continuously active deeds. The documents pertaining to the personnel, wage, and human resources shall be kept in a locked premise and a locked plate cabinet. The documents pertaining to the student status shall be kept in a locked premise and a locked filing cabinet, other documents pertaining to personal data shall be kept at least in a locked premise.
c) Archiving: Archiving shall be implemented pursuant to the University's records management and scrapping regulation and according to the archive plan.

USE OF ELECTRONIC MEANS IN PERSONAL DATA PROCESSING

Article 22. The detailed rules pertaining to the security of the use of electronic means in personal data processing, including the process for regularly testing, assessing, and evaluating the effectiveness of the measures for ensuring the security of processing shall be set out by the University's regulation pertaining to the information technologies.

PROCEDURE ON PERSONAL DATA BREACH

Article 23. (1) Personal data breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the personal data transmitted, stored or otherwise processed.

(2) If an employee of the University detects the suspicion of a personal data breach or the processor reports a data breach, the employee shall inform the data protection contact person of the unit without delay, who consults with the (health) data protection officer if necessary, and informs the head of the controller organisational unit without delay. The head of the unit shall decide whether the event is a breach or not. In the event of a breach, the data protection contact person enshrines its situations, especially the following

a) the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) the likely consequences of the personal data breach;
c) the measures that are taken or proposed to be taken by the controller unit to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
d) the measures that the data subject may implement to mitigate the possible adverse effects.

(3) The data protection contact person, in consultation with the head of the unit, makes a suggestion to assess the severity of the breach, which may be minor risk, probable risk or probable substantial risk, then notifies the (health) data protection officer within 24 hours about the breach and its situations as set out in subsection (2) herein. If there is missing information after the 24 hours, then all available information shall be provided.

(4) The (health) data protection officer shall decide about the severity of the breach and the following measures to be taken according to it and may request further information from the unit that possibly has further information about the breach.

(5) If the breach poses a probable risk to the rights and freedoms of natural persons, the (health) data protection officer proposes to the head of the unit to submit the case to the supervisory authority, then, according to the decision of the head of the unit, notifies the supervisory authority about the breach within 72 hours pursuant to the relevant legislation.

(6) If the breach poses a probable substantial risk to the rights and freedoms of the data subject or the cooperation of the data subject is required to mitigate the results of the breach and no relevant legal excluding conditions persist, the (health) data protection officer proposes without undue delay to the head of the unit to notify the data subject about the breach. The head of the unit, if assents, shall notify the data subject without undue delay. The notification shall contain the following at least

a) the nature of the breach and the scope of concerned personal data;
b) the name and contact detail of the (health) data protection officer or the contact person who is able to provide further information;
c) the information laid down in subsection (2) b)-d).

(7) The (health) data protection officer shall keep a record of the breaches for the University with the content set out in subsections (2)-(3) of Section 23.

(8) The controller organizational units shall keep a record of the types of the possible and eventual data breaches and shall inform the (health) data protection officer regularly about it.

CHAPTER VII.
THE MONITORING SYSTEM OF PERSONAL DATA PROTECTION TASKS OF THE CONTROLLER ORGANIZATIONAL UNIT

Article 24. (1) The heads of the organizational units shall monitor the compliance with the law and with the University's regulations, in particular, this Regulation, as part of their competence as head of the unit.

(2) In the event of a breach of the law, the head of the unit shall without due delay take measures to terminate the breach and shall submit to the competent employer of the Faculty or unit an action of infringement in order to determine liability.

(3) The head of particular organisational units (Faculty, independent organisational unit, patient care units of the Clinical Center, Directorate of the Chancellor, Chancellor's Office, Internal Monitoring Department) shall appoint a data protection contact person, who shall be in contact with the (health) data protection officer in the data protection matters, especially in the event of a data breach. A record containing the name and contact details of the data protection contact persons shall be kept by the Legal Department. In the event of a change in the person of this position, the head of the unit shall without undue delay notify the Legal Department.

(4) The head of any organizational unit and the data protection contact person may turn to the (health) data protection officer with questions in relation to the processing and regulation of personal data.

(5) The data subject, whose personal data is processed under the scope of this regulation may submit a complaint directly to the (health) data protection officer. The (health) data protection officer shall examine the complaint, inform the data subject about the result of the examination and make recommendations on the necessary measures to be taken by the controller organizational unit where appropriate.

LEGAL STATUS AND TASKS OF THE DATA PROTECTION OFFICER

Article 25. (1) The Chancellor shall appoint a data protection officer in order to comply with the legal and internal regulations pertaining to data processing and to ensure the enforcement of the rights of the data subjects. The person to be appointed to data protection officer shall have an appropriate level of

understanding of the legal regulation and application of the law pertaining to data protection, especially he/she shall have training, applied experience or scientific work in this field. After the expiration of the fixed term, the same person may be appointed again.

(2) The data protection officer may have other tasks, as long as these are not in conflict. Conflict may arise, in particular, from tasks that require decisions in relation to data processing (e.g. tasks of the head of the controller organizational unit).

(3) The data protection officer shall be professionally independent, only subordinated to the Chancellor, and he or she shall not be instructed. During the appointment of the data protection officer, the University shall not withdraw the appointment in relation to reasons emerging from the fulfillment of the tasks of the data protection officer, the data protection officer may not be sanctioned or fired, except when he or she conducts in a manner that termination with immediate effect would be adequate.

(4) The data protection officer shall receive a regular, monthly remuneration for his or her services. The University shall ensure the resources necessary to maintain the professional knowledge of the data protection officer.

(5) A data protection administrator acting under the professional guidance of the data protection officer shall assist him or her.

Article 26. (1) The data protection officer shall

a) give information and professional advice about the obligations set out in data protection regulations. In this regard, the data protection officer may adopt resolutions in particular cases or recommendations in general questions;
b) monitor compliance with data protection laws and University regulations in an order, intervals, and areas determined on his or her consideration;
c) cooperate in the increasing of the awareness of colleagues participating in data processing, organize training, take part in internal monitoring (audit) of personal data processing;
d) participate in the making and supervision of the records for data processing, and ensure that these registers are available at him or her;
e) give advice about the data protection impact assessment upon request, and monitor the carrying out of the assessment;
f) cooperate with the supervisory authority; in cases related to data protection, serve as a contact point for the supervisory authority, and have a consultative role in any other case in relation to data protection;
g) facilitate the exercise of the data subject's rights, thus examine the data subject's complaints and make recommendations on the necessary remedial measures, if needed;
h) participate in the making of the University's data protection regulation, and other regulatory provisions pertaining to data protection.
i) cooperate with the health data protection officer if needed.

(2) The data protection officer shall carry out his or her tasks adequately considering the risks connected to the data processing, with a view to the nature, scope, situation, and purposes of the processing.

(3) The University shall ensure that the data protection officer may join in on cases connected to his or her tasks in an adequate and timely manner, including the possibility to take part in discussions in these cases. The data protection officer shall be entitled to consultation of the data processing at every organizational unit in order to carry out his or her tasks. The data protection officer may ask for information from the head of the unit or from the employees of the unit. The person giving the information shall be responsible for the truthfulness of the information. The data protection officer shall be obligated to confidentiality in relation to the discovered data during his or her appointment, as well as after that.

(4) In case of a breach of the data protection regulations or a breach of law or in case of the hazard of it or in case of other jeopardy connected to the personal data, the data protection officer makes recommendations to remedy the breach, hazard or any other jeopardy. The data protection officer shall inform the head of the supervisory unit of the concerned unit and the higher leadership of the University and provide assistance to the restoration of lawfulness.

(5) The data protection officer shall make an annual report to the Chancellor until 31st January following the subject year.

THE HEALTH DATA PROTECTION OFFICER

Article 27. (1) The Clinical Centre shall appoint or commission a health data protection officer for a maximum of five years in order to organize and supervise the protection of data concerning health and patient care. The health data protection officer shall be a medic with specialist qualification or a person with legal studies with at least two years of practice or a person with health sciences studies with at least two years of practice in control of data concerning health. The same person may be appointed or commissioned after the expiration of the fixed term.

(2) The health data protection officer, in case of personal data concerning health, shall

a) give information and professional advice about the obligations set out in data protection regulations. In this regard, the data protection officer may adopt resolutions in particular cases or recommendations in general questions;
b) monitor compliance with data protection laws and University regulations in an order, intervals, and areas determined on his or her consideration;
c) cooperate in the increasing of the awareness of colleagues participating in data processing, organize training, take part in internal monitoring (audit) of personal data processing. Shall organize annual data protection training for the employees of the clinics, and shall organize regular training for the new employees and for the students; provides professional assistance for the consultation of data in scientific research concerning health;
d) participate in the making and supervision of the records for data processing, and ensure that these registers are available at him or her;
e) give advice about the data protection impact assessment upon request, and monitor the carrying out of the assessment;
f) cooperate with the supervisory authority; in cases related to data protection, serve as a contact point for the supervisory authority, and have a consultative role in any other case.
g) facilitate the exercise of the data subject's rights, thus examine the data subject's complaints and make recommendations on the necessary remedial measures, if needed.
h) participate in the making of the University's data protection regulation, and other regulatory provisions pertaining to data protection.
i) cooperate with the University's data protection officer if needed.

(3) The data protection officer shall receive a regular, monthly remuneration for his or her services. The University shall ensure the resources necessary to maintain the expert-level knowledge of the data protection officer.

(4) A health data protection administrator acting under the professional guidance of the health data protection officer shall assist him or her.

(5) Further rules pertaining to the legal status, tasks, and competence of the health data protection officer shall be laid down in the University's data protection regulation concerning health.

ENTRY INTO FORCE AND CLOSING PROVISIONS

Article 28. (1) This regulation shall enter into force on 25th May 2018. The former data protection regulation of the University that was adopted in 2007 shall be repelled with this regulation's entry into force.

(2) The organizational units shall appoint the data protection contact person and inform the Legal Department about the name and contact details of him or her until the 5th of June 2018.

(3) The organizational units shall make their data protection registers compliant with this regulation and send it to the (health) data protection officer until 31st October 2018.

Pécs, 23rd May 2018

Dr. József Bódis rector	Zoltán Jenei chancellor

Clause:

The regulation was adopted by the Senate on its 23rd May 2018 seating with the 55/2018 (05.23.) decision.