Kaposvár University
Privacy Policy

2018

Contents

Pursuant to EU Decree 2016/679 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 (General Data Protection Regulation), furthermore Act CXII of 2011. on information self-determination and freedom of information (hereinafter referred to as Infotv.), Act CCIV of 2011 on the national higher education (hereinafter referred to as: Nftv.), Govt. Decree 87/2015. (IV. 9.) on the implementation of certain provisions of the national higher education act (hereinafter referred to as: Vhr.), in accordance with other provisions of relevant legislation and university rules, the Senate of Kaposvár University (hereinafter referred to as University) shall create the following rules.

GENERAL PROVISIONS

1. § Scope, purpose

(1) The personal scope of the regulations covers all individuals employed by the University in the following legal statuses

a) public employment, management contract or other work agreements (public interest voluntary agreement, students' work agreement, doctoral student contract, hereinafter together: other work agreement statuses),
b) students (including auditing students), doctoral candidates
c) statuses not covered in items a)-b), participants of adult training programmes, courses organised, operated by the University (hereinafter together: adult education); applicants for doctoral degree obtainment procedures or participating in such; users of the library system of the University
d) statuses not covered in item a), applicants for habilitation procedures or participating in such,
e) furthermore, individuals using University infrastructure in connection with Sections 22-24. of the Regulations.

(2) The personal scope also extends to individuals who:

- though not in legal relationship, the University manages, or is obliged to manage pursuant to legislation, their data – either in order to establish such relationship or after the relationship is terminated,
- participate in University data processing activities in any capacity.

(3) The material scope of the regulations cover

- all data management and data processing activities,
- all data either personal, of public interest or accessible on public interest grounds, whether the management is performed with automated devices or manually.

University data management activities related to personal data are contained in the Data management records.

(4) The aim of the Regulations is to ensure that the management and protection of registries, data is carried out safely, pursuant to legislation, preventing unauthorised access to data, any alteration or disclosure thereof. Also, at institutional level, the regulation shall define the order of access to data of public interest generated at the University and establish the range of public information required to be published and fundamental security provisions.

(5) The scope of this regulation does not include technical data security in connection with IT devices, which shall be provided for in Kaposvár University IT Security Regulation (hereinafter: IBSZ).

2.§ Interpretative provisions

Pursuant to those laid down in 3.§ of Infotv.:

1. *data subject:* any natural person directly or indirectly identifiable by reference to specific personal data;

2. *personal data:* data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;

3. *special data*:

a) personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life,

b) personal data concerning health, pathological addictions, or criminal record;

4. *criminal personal data:* personal data relating to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

5. *data of public interest:* information or data other than personal data, registered in any mode or form, controlled by the body or individual performing state or local government responsibilities, as well as other public tasks defined by legislation, concerning their activities or generated in the course of performing their public tasks, irrespective of the method or format in which it is recorded, its single or collective nature; in particular data concerning the scope of authority, competence, organisational structure, professional activities and the evaluation of such activities covering various aspects thereof, the type of data held and the regulations governing operations, as well as data concerning financial management and concluded contracts;

6. *data public on grounds of public interest:* any data, other than public information, that are prescribed by law to be published, made available or otherwise disclosed for the benefit of the general public;

7. *the data subject's consent:* any freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations;

8. *the data subject's objection:* a declaration made by the data subject objecting to the processing of their personal data and requesting the termination of data processing, as well as the deletion of the data processed;

9. *controller:* natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor;

10. *data processing:* any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans);

11. *data transfer:* ensuring access to the data for a third party;

12. *disclosure:* ensuring open access to the data;

13. *data erasure:* making data unrecognisable in a way that it can never again be restored;

14. *tagging data:* marking data with a special ID tag to differentiate it;

15. *blocking of data:* marking data with a special ID tag to indefinitely or definitely restrict its further processing;

16. *data destruction:* complete physical destruction of the data carrier recording the data;

17. *data process:* performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;

18. *data processor:* any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions;

19. *data source:* the body responsible for undertaking the public responsibility which generated the data of public interest that must be disclosed through electronic means, or during the course of operation in which this data was generated;

20. *data disseminator:* a public body responsible for undertaking the public responsibility to upload the data sent by the data source if it has not published the data;

21. *data set:* all data processed in a single file;

22. *third party:* any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor;

23. *EEA Member State:* any Member State of the European Union and any State which is party to the Agreement on the European Economic Area, as well as any State the nationals of which enjoy the same legal status as nationals of States which are parties to the Agreement on the European Economic Area, based on an international treaty concluded between the European Union and its Member States and a State which is not party to the Agreement on the European Economic Area;

24. *third country:* any State that is not an EEA State.;

25. *obligatory organisational regulation:* internal data protection regulation accepted by a controller or team of controllers employed in several countries including at least one EEA country and approved of by the National Data Protection and Information Freedom Authority (hereinafter referred to as Authority), obligatory for the controller or team of controllers, which ensures the protection of personal data in the event of transmission to a third country by way of unilateral commitment of the controller or team of controllers;

26. *data breach:* illegal management or processing of personal data especially unauthorised access, alteration, transmission, dissemination, erasure (loss) or destruction or inadvertent destruction or damage. It contains the range of involved personal data, the range and number of subjects suffering data breach, the time, circumstances and consequences of the breach and measures taken to eliminate them, and other data specified in the jurisdiction prescribing data processing.

27. *Data protection:* the regulation of processing personal data (entirety of rules, procedures, tools, methods) in order to enforce the subject's rights.

28. *University Data Protection Officer:* an individual with higher education degree in law, economics, IT or similar qualification, appointed by the Rector or the Chancellor of the University. Furthermore, individual appointed based on their professional skills especially expertise at data protection law and practice as well as aptitude for the performance of tasks.

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

30. *Right of Access:* right empowering the holder to receive access to personal and special data processed in a given data file.

31. *Private use:* use of personal data for any purpose in the lack of authority specified in Section 4. of this regulation.

3.§ The Principles of Data Processing

(1) The main principle of processing personal data is purpose limitation.

(2) Personal data shall be processed for definite purposes, to exercise rights and fulfil commitments. Data processing shall remain compatible with its initial purposes in every stage; collecting and processing data shall be fair and lawful. (Principle of lawfulness and fairness)
(3) Processed data shall be limited to what is necessary and suitable in relation to the purposes for which they are processed. Personal data may be processed only to the extent and for the period of time necessary for the realisation of the purpose.
(4) The personal data shall retain this quality during processing until the contact with the subject is recoverable. Contact is recoverable with the subject if the controller has the technical conditions necessary for recovery.
(5) In the course of data processing the accuracy, integrity and – if needed for the purpose of data processing – up-to-dateness of the data shall be ensured, and that the subject remain identifiable only for the period necessary for the purpose of data processing.
(6) During data processing the appropriate safety of personal data shall be ensured by the application of technical or administrative measures – especially those establishing protection against unauthorised or illegal processing, inadvertent loss, destruction or damage of data.
(7) The controller is responsible for compliance with the principles of data processing, and shall also be able to verify this.
(8) In the course of data processing, access to public data and data accessible on public interest grounds, also the protection of personal data shall be ensured.

4.§ The legal basis of data processing

(1) No personal data may be processed without legal basis at the University.
(2) Personal data may be processed at the University if
a) the subject gave their written consent, or
b) it is ordered by law or – on the basis of enabling jurisdiction, within the scope specified therein – a municipality rule for a purpose based on public interest (hereinafter: mandatory data processing),
(3) Special data may be processed in cases described in Sections (4)-(10) and also if
a) the subject gave their written consent,
b) in the case of data specified in Info. tv. 3.§ 3. item a) it is necessary for the implementation of a promulgated international agreement, or it is ordered by law for the guarantee of a fundamental right laid down in the Constitution, for national security reasons, the prevention or prosecution of criminal acts, or home defence interests, or
c) it is ordered by law in case of data laid down in Info. tv 3. § 3. item b) for purposes based on public interest.
(4) In the event of mandatory data processing the types of data to be processed, the purpose and conditions of data processing the accessibility of the data, the period of data processing, the person of the controller are defined by the law or municipality rule ordering the data processing.
(5) Personal data may be processed if the consent of the subject is unobtainable or would involve disproportionate costs, and where the processing of personal data:

a) is necessary for compliance with a legal obligation to which the controller is subject, or

b) for the purposes of the legitimate interests pursued by the controller or by the third party or parties, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

(6) In the event of the subject's inability to give consent due to incapacity or other force majeure, their personal data may be processed in the necessary extent for the purposes of defending their own or other person's vital interests, preventing or eliminating immediate risks

threatening individuals' lives and physical integrity or material assets during the existence of the obstacles of the consent.
(7) If the purpose of consent-based data processing is the implementation of the contract concluded with the controller in written form, the contract shall contain all information relevant for the subject under the law in connection with the processing of personal data, especially the definition of data to be processed, the duration of data processing, the purpose of use, the fact, and the recipients of the data transmission and the fact of employing a data processor. The contract shall unambiguously contain that the subject has given their consent to the use of their data as specified in the contract by giving their signature.
(8) If the personal data is collected with the subject's consent, the controller, unless provided by law otherwise, may process the data:

a) for compliance with a legal obligation to which the controller is subject, or
b) for the purposes of the legitimate interests pursued by the controller or by the third party or parties, if the support of these interests is proportionate to the limitation of right to the protection of personal data without further contribution, furthermore, is allowed to continue processing after the subject has withdrawn their consent.

(9) The subject's consent shall be considered as given with respect to personal data communicated by them during public appearances or provided by them for the purpose of public disclosure.
(10) The consent shall be presumed in proceedings launched on the subject's application or on their initiative, with respect to personal data necessary for conducting the proceedings, while in other actions launched on the subject's application, with respect to personal data provided by them.
(11) In the event of ambiguity the subject's refusal of giving their consent shall be presumed.

5.§

(1) Based on the principle of purpose limitation, data processed in individual procedures may only be used for the purpose of the implementation of the given case and may not be linked to other procedures or data; unless permitted by law or the subject has given their consent, and the conditions of data processing are valid for each and every personal data.
Further data processing for the purposes of archiving for public interest, scientific and historical research or statistics shall be considered as compatible, lawful data processing operation.
(2) The University may keep records of data indispensable for orderly operation, the pursuance of employer's rights and the organisation of training programmes, furthermore those necessary for the assessment and verification of entitlement to facilities provided by legislation and the organisational and operational regulation. For this purpose data containing the right owner's identity and their entitlement to the facility may be processed.
The University is entitled to process data belonging to employees, students and individuals participating in programmes without student status only with valid legal basis, with the establishment and performance of employment, fees, facilities and obligations, with regards to the pursuance and the fulfilment of citizen's rights and obligations, for national security reasons, for the purpose of managing registries defined in the national higher education act, to an extent adequate for the purpose, limited to the purpose. The employees' personal data – unless provided otherwise by social security rules – may be processed for five years from the termination of the employment. Students' personal data remain open for processing for eighty years from the notification of termination of the student status.
(3) If the data processing is based on the subject's consent, the purpose of data processing shall be defined by the head of the administrative unit in their field of operation.
(4) If any unavailable information necessary for the arrangement of an issue or fulfilment of a task – in case of personal or classified information, open for processing under the law – is

obtainable from a primary information source, the University shall obtain it – unless provided otherwise by legislation – from the primary information source by electronic means.
(5) Personal data collected for the purpose of scientific research may only be used for scientific research. The recognition of the relationship of the personal data with the data subject – as soon as allowed by the research goal – shall be made permanently impossible, but until then the data suitable for the identification of an identified or identifiable individual shall be stored separately and may be linked to other data only for the purposes of the research. The body or individual performing the research may disclose personal data only if the data subject has given their consent or it is necessary for the presentation of the results of a research about historical events. While using personal data in the course of a research, the leader of the research shall be responsible for compliance with the data protection rules, and is obliged to ensure that the participants seek to observe the data protection and data security rules of the research. If students also participate in the research, or, in the course of publicising the results and the process of the research for educational purposes, disclosure of personal data to students cannot be by-passed, it shall be the responsibility of the leader of the research and the teacher involved to lecture the students on the data protection and data security rules and enforce them. In the interpretation of this rule research carried out with the participation of students also applies to the preparation of the dissertation of a doctoral student, in which case the supervisor shall be responsible for lecturing the student on the data protection and data safety rules and enforcing thereof. A record of lecturing the students on the data protection and data security rules shall be drawn up and undersigned by the teacher, the researcher and the students.
(6) Personal data processed in the framework of mandatory processing – unless provided otherwise by law – may be taken over by the Central Office for Statistics for statistical purposes in a way that allows the identification of individual information, and may process them as specified by legislation. Personal data collected, transferred or processed for statistical purposes – unless provided otherwise by law – may be processed only for statistical purposes as law provides; and the personal data shall be transferred for statistical purposes so that it cannot be linked to the data subject. It follows from the statistical purpose that the result of statistical data processing cannot be personal data but aggregated data, and this result or the personal data will not be used to support measures or decisions referring to specific individuals.

6.§ The University Organisation of Data Protection, Data Security and data processing. Data Protection Officers

(1) The heads of the administrative units, the University Student Union and its divisions, the University Doctoral Student Union and the presidents of the faculty doctoral student agencies shall ensure that the rules laid down in this document are observed.
(2) The head of the institute of public education maintained by the University shall ensure that this regulation be applied appropriately to individuals employed by them either in public employment, work contract or student status.
(3) Technical data protection related to IT tools is the responsibility of the IT Department of the Services and IT Directorate as specified in IBSZ.

7.§

(1) The University Data Protection Officer may fulfil their tasks as an employee of the controller or the processor or in the framework of a service contract (they may be responsible for other tasks, but care must be taken that these tasks do not generate a conflict of interests). Regarding the performance of their duties, they are bond by the obligation of secrecy and the confidentiality of data.
The controller and the processor shall provide resources necessary for fulfilling their tasks and ensure that they accept no instructions from anyone with regards to the fulfilment of their tasks;

the Officer is answerable only and directly to the top management of the controller and the processor.

(2) The University Data Protection Officer shall:

- provide contribution and support to making decisions related to data procession and the safeguarding of data subjects' rights;
- control the observation of provisions of legislation and University data protection and data security regulations as well as data security requirements. In the framework thereof they may require information and check the practice of data procession, have insight into any record, document connected to data protection;
- investigate reports and in the event of detecting unauthorised data processing, call the controller or processor to eliminate the problem (replace or correct data damaged, modified or erased due to unauthorised act) and shall notify the Rector and the Chancellor. The Officer shall keep a complaint management record in this respect (Annex 15.);
- draft the University data protection and data security regulation;
- keep the Data protection registry (Annex 3.);
- provide for education on data protection knowledge;
- cooperate with the supervisory authorities and report data breach without undue delay – not later than 72 hours after having become aware of it (otherwise attach justification of delay) – to the Authority as shown by Annex (1.a) unless the University can prove that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. They shall notify the data subject without undue delay – in close cooperation with the Authority and observing their or other involved authorities' instructions – if the data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to take the necessary cautionary measures.
- represent the University at the conference of internal data protection officers;
- participate in a consultative capacity in forums discussing data protection topics.
- keep the records of the appointed data protection officers of the administrative units
- keep a university data breach registry to control measures taken in connection with detected data breaches and to notify the data subject (Annex 1.).

(3) Faculties, directorates and the institute of public education shall appoint at least one territorial data protection officer each (hereinafter together: territorial data protection officer) from the employees of the University. In the case of faculties, the Rector, in the case of the directorates, the Chancellor, in the case of the institute of public education, the head of the institute shall appoint the territorial officer. One employee may be the territorial officer of several administrative units at the same time, and one unit may employ several officers. In this case the appointment letter shall accurately describe which territories belong to the officer in question.

(4) The territorial data protection officer especially shall:

- follow an annual work plan to control the data management and data procession activities performed at the unit belonging to their territory and in the course thereof inspect letters and documentation related to data protection
- control the legality of data transmission (application – public data, other – and measures), and keep a data transmission record for the unit in order to notify the data subject (Annex 2.), which shall be forwarded to the University data protection officer at the end of every month;
- immediately report any data breach to the University data protection officer that happened or was detected in the unit belonging to their territory (Annex 1.), and initiate the modification of the data processing registry (Annex 3.).
- draw the university data protection officer's attention to data protection and data security-related issues,

- cooperate in the regulation of access to electronically processed data and the drafting and amendment of the University data protection and data security regulation,
- participate in consultative capacity at forums of the administrative unit if data protection-related topics are discussed,
- prepares data subjects' applications for access to data, erasure, prohibition of processing data and forwards them to the head of the administrative unit. Keeps records in connection with the foregoing.

8.§

(1) The university/territorial data protection officer shall not substitute but support and coordinate data processing related duties, personal responsibilities in connection with observing data protection standards of the heads and staff of administrative units.
(2) In the event of detecting any breach of law concerning the data protection regime, the head of the administrative unit shall, in cooperation with the territorial officer, immediately take measures to eliminate it. Should the measure fail, the rector and the chancellor shall be notified through the University officer, who, in case of particularly serious abuse, shall initiate the establishment of liability, compensation procedures where applicable, and arrange for restoring the legal status.
(3) The rector and the chancellor of the university have, with prior notification of the head of the administrative unit, unlimited right, vice rectors and heads of administrative units (including presidents of boards) have rights restricted to their field of competency of inspection into the data protection of administrative units. Heads may transfer their rights of inspection to other individuals. Obligation of secrecy applies to all personal data accessed in the course of inspection.
(4) Data processors and individuals covered in 1.§ of this regulation shall preserve all personal data accessed and processed by them as confidential information of the institution, and make all possible effort to ensure proper protection thereof. Only individuals who have made a declaration of secrecy may be employed in such position (Annex 13-14.).
If this individual, based on their position or rank, has access to or gains possession of personal, special or criminal data, they shall act as provided in Infotv., especially use personal data only for the previously fixed purposes and protect the data from unauthorised access.
Using personal data processed by the university-– or obtained from other controller to fulfil tasks for the university – for private purposes is prohibited. Any employee violating this provision commits disciplinary offence.
(5) The data controller shall bear disciplinary, compensation, administrative and criminal responsibility for the lawful management of all personal data accessed in the exercise of their powers and the legitimate exercise of rights of access available for the university registries.
(6) If the controller becomes aware that the data under their management is incorrect, incomplete or untimely, they shall correct it or initiate correction with the staff member responsible for recording the data.
(7) If the University concludes a contract with a third party for a purpose other than data processing, but in the course of performing the tasks personal data management is realised, the contract shall stipulate the obligation to observe the provisions of relevant legislation, this regulation and the IBSZ.

9.§ The requirements of data security

(1) Data security: the totality of organisational, technical solutions and procedural rules against unauthorised management of personal data, especially access, processing, alteration and erasure thereof; a status of data management where risk factors – threat included – are minimised by organisational, technical solutions and arrangements.

(2) Controllers shall make arrangements for and carry out data processing operations in a way so as to ensure full respect for the right to privacy of data subjects in due compliance with the provisions of this Act and other regulations on data protection. Among several possible data management tools the one providing the highest level of protection shall be selected unless posing disproportionate difficulties for the controller.
(3) Controllers, data processors must implement adequate safeguards and appropriate technical and organizational measures (with regard to the current standard of technology) to protect personal data, as well as adequate procedural rules to enforce the provisions of Infotv. and other regulations concerning confidentiality and security of data processing. Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technology.
For the protection of data sets stored in different electronic filing systems, suitable technical solutions shall be introduced to prevent – unless this is permitted by law – the interconnection of data stored in these filing systems and the identification of the data subjects.
(4) Necessary measures shall be taken to safeguard both manually and digitally stored and processed data. Protective measures shall be proportionate with the threat and the danger of abuse.
(5) In respect of automated personal data processing, data controllers and processors shall implement additional measures designed to:

a) prevent the unauthorized entry of data;
b) prevent the use of automated data-processing systems by unauthorized persons using data transfer devices;
c) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data transfer devices;
d) ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;
e) ensure that installed systems may, in case of malfunctions, be restored; and
f) ensure that faults emerging in automated data-processing systems is reported.

By exclusively automated data processing, a decision based on the assessment of the data subject's personal characteristics may be made only if the decision is made for the conclusion or the performance of a contract or if the decision is authorized by law that safeguards to protect the data subject's legitimate interests are in place, or the data subject has given their explicit consent. In the event of such a decision, the data subject shall, on request, be informed on the applied method and its essence, also, must be granted opportunity to express their position or lodging in an objection.
(6) The disclosure of any personal data processed at the University is prohibited unless so ordered by law. Students' grades, exam results and the fact whether they receive any social benefits are personal data; in the event of disclosure, codes instead of names are applicable.
(7) In case of special data greater care shall be exercised; proper technical and administrative measures shall be taken to ensure that in the course of performing data processing operations special data are accessible only for staff for whose data processing related task they are strictly necessary.

10.§

(1) To safeguard *personal data stored on computers or networks* the following measures are to be taken:
a) mirroring: the principal database of the network server machine (hereinafter: server) containing personal data shall continuously be mirrored on a physically separate database.

b) backup: active data of databases containing personal data shall be saved on a separate medium as a safety backup at least once a week. The medium containing the safety backup must be guarded in a way guaranteeing high data security.
c) archiving: the passive proportion of databases containing personal data – sets needing no more processing and remaining unaltered – shall be separated from the active part and the deactivated data shall be stored on a separate medium.
d) fire protection: the server shall be kept in a safely lockable, air conditioned room equipped with fire protection and safety alarm system.
e) power supply: the power supply of the server shall be equipped with a UPS, which, in the event of power outage, provides smooth operation for the period necessary for a safe system shutdown.
f) virus protection: a virus protection software shall run non-stop on the server. Disinfection shall continuously be ensured on every user's desktop or networked portable computer (hereinafter: work station).
g) access protection: Network resources are accessible only with valid usernames and passwords. The replacing of passwords shall regularly be taken care of. The passwords of the system manager and the administrator users shall be replaced by the head of the workplace at specified intervals. Current passwords shall be kept in places protected from unauthorised access, and the head of the workplace shall be provided documented access to them any time.
(2) For the security of *personal data processed manually*, the following measures are to be taken:
a) fire and property protection: archived documents shall be stored in safely lockable, dry room equipped with fire protection and safety alarm system.
b) access control: only competent administrators may have access to processed data. Data concerning personnel, wages and labour shall be stored in reinforced safes, those related to student status shall be stored in a reinforced safe in a separate lockable room. Consignments containing classified data may be opened only by the rector or the chancellor, or a deputy entrusted with this task by them.
c) archiving: archiving of the documents of data processing shall be carried out once a year. Archived documents shall be sorted out and deposited in the archive in compliance with the University records management policy and the archive plan.
(3) The detailed definition of IT security provisions, the classification of data processed at the University into security classes, the rules of security requirements are contained in IBSZ, while the data management rules of records are described in the records management policy.

11.§ Data Protection

(1) Records or media containing personal data may leave University grounds only in duly justified cases, with the explicit approval of the head of the administrative unit in question. In this case the employee holding the record or media shall be responsible for its safekeeping, integrity and blocking any unauthorised access. No records containing special data and state or business secret are allowed out of the institution.
(2) Individual staff members are allowed to pursue data management activities only to the extent necessary for fulfilling their scope of work. Staff performing data management shall ensure the safety of the data and records processed by them.
(3) Records containing personal data shall be stored in locked rooms. In worktime, staff shall take particular care of the security of their offices and tools used for storing records and data. Computers must be turned off and offices must be locked when worktime is over. Staff must handle and store computers and jointly used data media to block out unauthorised access.
(4) Entities in legal relationship with the university shall arrange the management, storage of intellectual property, research results, learning material, invention, etc. mainly with tools of the

University, in case of university IT service in compliance with the provisions of IBSZ. If data of this nature is processed outside the University, staff shall ascertain whether the provisions of this regulation are enforceable.
(5) The order of protection against fire is contained in the University work and fire safety regulations.
(6) Staff may use University computer infrastructure only in accordance with its intended purpose. The tools must be used for activities detailed in the job description.
(7) Right of access to individual folders of the University file servers and the right to use intranet outside the University is granted by the controller. The order of providing the right of access and the rules of registry are contained in IBSZ.
(8) Staff shall take extra care to block unauthorised access to the passwords for University systems. In this context
a) passwords must be modified every six months, must be designed impossible to guess and must not be given out.
b) terminals, work stations logged into any system shall not be left unattended without logging out,
c) staff shall not use other staff members' resources without authority,
d) it is forbidden to break technical restrictions protecting network resources or to obtain other users' passwords, and
e) it is forbidden, outside regular worktime, to copy, delete or modify data and files of the system or other users without permission.
(9) The central network and the individual work stations are protected with a firewall and a regularly updated antivirus software, the operation and updating of which is the responsibility of the IT Department.
(10) The physical protection of the electronic data storage devices shall be properly ensured, that is they shall be kept in locked, protected rooms, no food or drink shall be consumed near the IT tools, and staff may take only computers protected with passwords out of University grounds with strict inventory liability.
(11) In order to render the lawfulness of electronic data management operations with personal data verifiable, the University records the following in an automated data management system (hereinafter: electronic diary):
a) the definition of the range of personal data involved in data management,
b) the purpose and cause of data management operation,
c) the exact time of the performance of the data management operation,
d) the identification of the person carrying out the data management operation,
e) in the event of transmission of personal data, the recipient of the transmission.
The data recorded in the electronic diary may be open to access and use only in order to check the lawfulness of data management, to enforce data security requirements or to conduct criminal proceedings. Recorded data shall be preserved for ten years after the deletion of the managed data.

12.§ Preliminary information of the data subject

(1) Prior to data processing being initiated the data subject shall be informed whether his consent is required or processing is mandatory, the purpose for which his data is required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, and the persons to whom his data may be disclosed (recipients). Information shall also be provided on the data subject's rights and remedies.
(2) In the case of mandatory processing such information may be supplied by way of publishing reference to the legislation containing the information referred to in Subsection (1).

(3) If the data management is based on consent, the controller shall certify that the subject has given their consent to the management of their personal data and whether the consent was given on a voluntary basis. If the subject's written declaration also covers cases other than this, the application for consent shall be arranged in a way clearly distinguishable from the other cases. The subject is entitled to withdraw their consent at any time, and they shall be informed about this before giving the consent. The withdrawal of the consent shall be the same simple as giving it. The withdrawal of the consent shall not affect the lawfulness of the consent-based, pre-withdrawal data management.
(4) If the provision of personal information to the data subject proves impossible or would involve disproportionate costs, the obligation of information may be satisfied by the public disclosure of the following:

a) an indication of the fact that data is being collected;
b) the data subjects targeted;
c) the purpose of data collection;
d) the duration of the proposed processing operation;
e) the potential data controllers with the right of access;
f) the right of data subjects and remedies available relating to data processing; and
g) where the processing operation has to be registered, the number assigned in the data protection register, with the exception of Subsection (2) of Section 68 of Infotv.

(5) The information for the data subject described under Subsection (1) – depending on their relationship with the University – shall be provided by the controller involved with the content described and the method defined in Annexes 7-12., and the information files shall be uploaded to the University homepage. Information shall be provided in Hungarian, for non-Hungarian speakers in English.
(6) If the controller wishes to perform further data processing on the personal data for purposes other than their collection, they shall notify the subject about this purpose and all other relevant supplementary information prior to operations.
(7) The possibility of preliminary information is provided for the subjects by the University through the regulations available on the homepage. It is an obligatory content element of the students' registry sheet and the work contracts that the other party shall acknowledge getting acquainted with the provisions of the relevant University regulations.

13.§ The data subject's rights and their enforcement

(1) The subject is entitled to request the controller for information on the management of their personal data and also has the right of inspection into them. Inspection shall be provided so the subject may not have access to other individuals' data. The subject's right extends to requiring rectification and – except mandatory data management – erasure or blocking of their personal data.
(1a) The subject is entitled to have their personal data they allowed a controller access to in a format widely used and readable on computer, and also has the right to transmit these data to another controller without being hindered by the controller they previously made the personal data available for if the data management is based on consent or a contract, and the data management takes place in an automated way. This right may not adversely affect other individuals' freedoms and rights; and may not be applied in case the data management is for public interest or it is indispensable for the fulfilment of tasks that the controller performs in the context of exercising the public powers they are entrusted to.
In the course of exercising their right to data portability, the data subject is entitled – provided it is technically feasible – to request the transmission of their personal data directly between controllers.

(2) Upon the data subject's request the data controller shall provide information concerning the data relating to him, the sources from where they were obtained, the purpose, grounds and duration of processing, the circumstances, effects of an accidental data breach and measures taken to eliminate it, and - if the personal data of the data subject is made available to others - the legal basis and the recipients (also in the event of employing a processor, the name and address of the data processor).
(3) Data controllers must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than thirty days. The information shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. The amount of such charge may be fixed in an agreement between the parties. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.
(4) The data controller may refuse to provide information to the data subject in the cases defined under Subsection (1) of Section 9 and under Section 19. Should a request for information be denied, the data controller shall inform the data subject in writing as to the grounds for refusal. as well as the possibilities for seeking judicial remedy or lodging a complaint with the Authority.
(5) Where a personal data is deemed inaccurate, and the correct personal data is at the controller's disposal, the data controller shall rectify the personal data in question. In the event of detecting data alteration or incorrect data recording the subject shall initiate the rectification or correction of their data under processing, which the controller shall carry out within five days.
(6) Personal data shall be erased if:

a) processed unlawfully;
b) so requested by the data subject in accordance with Paragraph c) of Section 14;
c) incomplete or inaccurate and it cannot be lawfully rectified, provided that erasure is not disallowed by statutory provision of an act;
d) the purpose of processing no longer exists or the legal time limit for storage has expired;
e) so ordered by court or by the Authority.

The erasure shall carried out within five days except the case described in Paragraph d), where the requirement of erasure shall not apply to personal data recorded on a carrier that is to be deposited in archive under the legislation on the protection of archive materials – and the fact of this shall be officially recorded.
(7) Personal data shall be blocked instead of erased by the controller if so requested by the data subject, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure. The data of the subject may not be erased if the data processing was ordered by law, but the data may not be transmitted to the recipient if the controller agreed with the objection or the court established the lawfulness of the objection.
(8) The controller shall tag the personal data processed by them if the subject disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed data cannot be unambiguously established.
(9) When a data is rectified, blocked, marked or erased, the data subject and all recipients to whom it was transmitted for processing shall be notified. Notification is not required if it does not violate the rightful interest of the data subject in light of the purpose of processing.
(10) If the data controller refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request

for rectification, blocking or erasure is based shall be communicated in writing or, on the consent of the data subject, electronically within thirty days of receipt of the request. Where rectification, blocking or erasure is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.
(11) The data subject shall have the right to object to the processing of data relating to him
- if processing or disclosure is carried out solely for the purpose of discharging the controller's legal obligation or for enforcing the rights and legitimate interests of the controller, the recipient or a third party, unless processing is mandatory;
- if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and
- in all other cases prescribed by law
In the event of objection, the controller shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision.
(12) If, according to the findings of the controller, the data subject's objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.
(13) If the data subject disagrees with the decision taken by the controller under Subsection (10), or if the controller fails to meet the deadline specified in Subsection (10), the data subject shall have the right under Section 22 to turn to court within thirty days of the date of delivery of the decision or from the last day of the time limit.
(14) If data that are necessary to assert the data recipient's rights are withheld owing to the data subject's objection, the data recipient shall have the right under Section 21 Subsection (3) of Infotv. to turn to court against the controller within fifteen days from the date the decision is delivered under Section (22) of Infotv. in order to obtain the data. The controller is authorised to summon the data subject to court.
If the data controller fails to send notice as specified in Subsection (3), the data recipient shall have the right to request information from the controller concerning the circumstances of non-disclosure, upon which the controller shall make available the information requested within eight days of receipt of the data recipient's request. Where information had been requested, the data recipient may bring an action against the controller within fifteen days from the date of receipt of the information, or from the deadline prescribed therefor. The controller is authorised to summon the data subject to court.
(15) In the event of a breach of their data processing related rights, the subject may turn to the University data protection officer or to court, initiate an investigation at the National Data Protection and Information Freedom Authority demanding compensation for damages and grievances. The University data protection officer shall examine the complaint and if has reasonable grounds, initiates measure at the head of the unit. Otherwise the officer shall reject the complaint and notify the complainant in written form within 30 days from the delivery of the complaint on the factual and legal reasons of the rejection and inform them of the possibilities for seeking judicial remedy or lodging a complaint with the Authority. If the court grants the application, the controller shall be ordered to provide the information, rectify, block, erase the data, destroy the decision made through automated processing, take the subject's right to objection into consideration and release the data requested by the receiver.
(16) If data controllers cause damage to a data subject as a result of unlawful processing or by any breach of data security requirements, they shall pay for such damages. If the data controller, by unlawful data processing or by breaching data security rules, violates the personal rights of the data subject, the latter may demand restitution from the data controller. The controller shall

be released from liability for damages and from paying restitution if s/he demonstrates that the damage or the violation of personal rights were brought about by reasons beyond his/her data processing activity. No compensation shall be paid and no restitution shall be demanded where the damage or the violation of rights was caused by intentional or serious negligent conduct on the part of the aggrieved party or the data subject.
(17) The University as data controller is entitled to obtain compensation against an employee in public employment or work contract who, by breaking data processing regulations, causes damage within the legal status of their employment. The amount of damage demanded may not exceed the public employee's or work contractor's four months' work stoppage fee. In the event of damage caused by intentional or serious negligent conduct the total damages shall be reimbursed. In questions not regulated here, provisions of Act I of 2012. on Labour Code, Act XXXIII of 1992. on the legal status of public servants (hereinafter: Kjt) and the internal regulations of the University shall govern.

DATA TRANSMISSION. INTERCONNECTION OF DATA PROCESSING OPERATIONS

14.§ Common rules of data transmissions

(1) In the course of transmitting personal data, when that takes place as a mail consignment, care must be taken that the consignment is posted closed. In the course of transmitting personal data protective measures laid down in IBSZ must be taken.

15.§ Interconnection of data processing operations. Data transmission

(1) Data processed at individual administrative units specified in Annex 3 of Nftv. are connectable within the university if necessary. Interconnection with other controller's data is possible where appropriate and only if the subject has given their consent or it is allowed by law and the conditions of data processing are met for each and every personal data.
Interconnection of data processing shall be reported by controllers to the University data protection officer on the data form in Annex 5., which contains the following:

- the names of the interconnected data processing operations,
- the purpose and designation of the interconnection,
- the time and duration of interconnection,
- its legal basis (University regulation supporting the fulfilment of law, statutory provisions)
- the interconnector's name, position, unit, office, phone number,
- range and number of individuals involved in the interconnection,
- scope of interconnected data,
- method of interconnection (manual, computer, mixed)
- data security measures.

(2) Within the administrative system of the University, the data listed in Annex 3. of Nftv. – to the extent and for the period necessary for the completion of the task – may be transmitted only to units fulfilling administrative and organisational tasks in connection with employment and student status. If there is dispute between the two units about the data transmission, their common administrative superior shall decide.
Data listed in Annex 3. of Nftv. may be transmitted to external bodies disregarding the subjects' declarations in compliance with the provisions specified there. The competent controller shall notify the University officer about such data service quarterly.
(3) Non-statutory, non-mandatory transmission within the university shall be officially recorded in the unit performing the transmission, and shall be reported to the University officer. The registry contains the time, legal basis and recipient of the data transfer, the range of transferred data and other data provided by legislation.

Any request arriving from bodies or individuals outside the university for the purpose of data communication – except mandatory data service listed in Annex 3. of Nftv. – may be met only if the subject gives the University their written consent or if allowed by law; and the controller must make sure that the conditions of data processing are met for each and every personal data. The subject may give a prior consent of such content, which may apply to a period of time, a specified range of bodies submitting requests and the scope of transferable data.
It shall be considered as the student's unambiguous consent if the appropriate declaration is made on the special portal established in the electronic education system (Neptun). With respect to individuals holding public employment, work contract or other work-related legal relationship or student status with the University who submit an application to an external call through the University, the submission of the application shall be considered as their unambiguous consent that the university may transfer the tender-related personal data to the principal and the body entitled to control the submission, implementation and accounts of the projects.
(4) The protocol of the request and the copy of the reply given shall be stored at the place where the data were processed. All data concerning requests arriving from national security services – pursuant to Act CXXV of 1995 Section 42. – qualifies a state secret, of which no other bodies or individuals may be informed.
(5) If the data processing body or the controller receives a request for such data the legality of which they cannot assess, they shall notify the University officer.

16.§ Data transmission to the Higher Education Information System (FIR)

(1) The chancellor shall authorise the contact person with FIR on behalf of the Office of Academic Affairs and verifies the institutional data service with an electronic signature. The verification of the electronic data communication for FIR shall be carried out with the contact person's electronic signature generated for administrative purposes (of at least advanced or other security level specified by statutory provisions) or, based on the agreement concluded with the operator of the Central Electronic Service System, in a system secured by the Client Gateway.
(2) The contact person shall report the student's or doctoral candidate's personal data to FIR within fifteen days from the establishment of the student or candidate status; in the event of changes in these data, they shall report the modification within fifteen days from recording them in their own registry. Data of certificates, diplomas, supplements and obtained doctoral degrees issued after finishing higher education studies shall be reported to FIR within fifteen days from issuance. Relevant data of students in legal relationship with the dormitory, modification thereof, the establishment and termination of legal status and modifications in the students' data shall be reported to FIR within fifteen days from their occurrence.
(3) The contact person's other report obligations to FIR:
- personal data of staff employed in lecturer, researcher and teacher status (hereinafter: educators) and other employees within fifteen days from the establishment of the legal status;
- modification in educators' personal and employment data within fifteen days from recording in the contact person's own registry;
- in the event of the termination of the educator's employment within fifteen days from the termination of the status.

17.§ Data transmission in institutes of public education

(1) The data service obligation provided and specified by statutory law as regards the public education institute maintained by the university shall be fulfilled by staff appointed by the head of the institute. The head of the institute shall inform the University data protection officer about the name and position of the individual responsible for the data service in a written form.

18.§ Data transmission for abroad

(1) Transfer of data to EEA Member States shall be considered as if the transmission took place within the territory of Hungary. Data (including special data) may be transferred to a third country if the data subject has given his explicit consent and has received prior information about possible risks arising from the data transfer, or it is allowed by statutory law, it is necessary for important public interest, or the conditions laid down in GDPR Decree Section 49. and Infotv. and if the adequate level of protection of the personal data have been ensured in the third country during the course of the control and processing of the data transferred.
(2) Personal data may be transferred to third countries in the interest of the implementation of an international agreement on international legal aid, exchange of information in tax matters and on double taxation, for the purpose and with the contents specified in the international agreement.
(3) In the event of data processing where data transmission for abroad is foreseen, the subjects' attention must be called to this circumstance before collecting the data.
(4) Facts and circumstances regarding outbound data service shall be documented as described in Annex 2., one copy of which shall be stored at the place where the data processing took place for ten years and then deposit in the archive.

CUSTOM DATA PROCESSING

19.§ Student records

(1) The student registry is the processing of data regarding student status pursuant to provisions of statutory law (mainly Nftv., Vhr.) and university regulations.
(2) The data of student registry may be used for the fulfilment of organisational and administrative tasks in a defined scope, mainly the establishment, modification and termination of student status, the students' completion of their academic and exam obligations, the establishment and payment of benefits, the imposing, payment and collection of fees, as well as purposes defined by the data subject.
(3) For the purpose of the student registry, the University operates an electronic education system (hereinafter: Neptun), the university level coordination of the work of organisations cooperating in the operation, development, maintenance of which is the responsibility of the Directorate of Students' Affairs (DSA). The central administrative tasks not supported by Neptun shall be performed with other IT systems.
(4) The student registry contains the data of all the students of the university. Data listed in Nftv. Annex 3 I/B shall be collected from individual students.
(5) The data are provided by the admission database and the registry sheet filled in by the student. The data of individuals cooperating in the fulfilment of academic and administrative tasks shall be uploaded to the system by the administrative units based on their own registries. The collection of data to be entered in the database shall be conducted in writing (electronic or paper based). No data shall be entered in Neptun by verbal communication.
(6) Data processed in the admission process of applicants not admitted to the university after the admission process or are admitted to the university but fail to establish student status shall be erased six months after the end of the admission process.
(7) Figures entered in Neptun shall not differ from the data in the data source; the sameness of data is the responsibility of the individual performing the data entry. If the data contained in the document serving as the data source is uninterpretable, illegible, contradictory or incomplete, the data shall not be entered in Neptun, but the subject or the issuer of the original document shall be requested to make correction or completion of the data source.
(8) The controller of the student's data is the DSA and appointed staff at the faculty(ies) according to the student's programme. Furthermore, the student's data are processed by:

- appointed staff of the University Dormitories in the function related to dormitory membership;

- appointed staff of the University Library regarding data in connection with the use of the library and the library system;
- appointed member of the University Student Union or the University Doctoral Student Union regarding data of students working in cooperation with the union and data generated in connection with the fulfilment of tasks of their competence;
- appointed staff of the Department of Finance regarding financial affairs;
- educators announcing and running the courses visited by the student in the scope and to the extent of their function.

The allocation of the rights of access is the responsibility of the DSA so that the controllers can process and read the data only of students belonging to their sphere of competence.

(9) Data controller bodies may transfer data only with the permission of the accountable head of the body, by observing the provisions of the regulation. The data transfer shall be initiated by filling in the form in Annex 2. a). On assessing the lawfulness of the data transfer it is to be considered whether the body requesting the data is entitled to the processing of the data in question.

Administrative units within the University eligible for data transfer from Neptun are only those competent to establish academic and exam obligations, available social and other benefits, services (e.g. library, dormitory) and payment obligations concerning students.

(10) The provisions of this section (1)-(9) shall be applied with the following differences with respect to the participants of adult education trainings organised and run by the University and individuals not in employment status – pursuant to 1. § of this regulation – with the University but applying for or participating in habilitation procedures and doctoral degree obtainment procedures:

- applicants for doctoral degree obtainment procedures in Neptun,
- in other cases on paper basis or applying other software operated by the controller,
- regarding invoicing in adult trainings, the registry of payments and the issuance of invoices shall be realised with an established computer programme at the Department of Finances.

The operation and data processing of the graduate career tracking system shall be regulated by Annex 21. of the Kaposvár University Organisational and Operational Regulation (hereinafter: KE SZMSZ) vol.I, while Annex 23. contains provisions for the operation and data processing of the Alumni system.

(11) The data of the digital education system shall be protected against unauthorised access, alteration, transmission, disclosure, erasure or destruction as well as inadvertent destruction and damage. To ensure this protection is the responsibility of the system operator (IT Department), the DSA and staff and units performing data control and processing.

(12) The system operator shall take and maintain a high standard of the following measures for the security of the data stored on the servers:

a) store the servers in closed rooms equipped with adequate physical protection. Ensures the environmental and technical conditions of the operation of servers;

b) generates safety backups of the active data of databases containing personal data on a daily basis. The backup an d the active database shall be stored on media situated at separate sites;

c) ensures that the servers containing personal data are not accessible via direct network contact and system intrusion is impossible through network access;

d) ensures that in the event of power outage servers can be shut down smoothly and without data loss;

e) provides for the virus protection of servers;

f) in case the database server is accessed through terminal servers, the operator provides for the allocation and withdrawal of IDs and passwords needed for login to terminal servers and the setting of access rights minimally adequate for the purpose of data processing;

g) the system manager's password for the server and the IT system must be locked inside a fireproof metal box. The changing of passwords shall be carried out at least once every six months.
(13) Neptun shall be allowed to log the fact, time and operator of data modifications.
(14) Further rules concerning student registry are laid down in Nftv. and Vhr., also KE SZMSZ vol.III.

20.§ Employee records

(1) Employee records are data processing for the documenting of facts related to public employee status, employee status, work contract, with the statutory support of Nftv, Kjt, Mt., their implementing regulations and KE SZMSZ.
(2) The data of the employee records are available for the establishment of employment-related facts, certifying classification requirements, payroll management, social security administration and statistic data service.
(3) The employee records contain the data of all employees of the university either in public employment or any other legal status.
(4) The data of the employment records are provided by the data subject. The primary data collection takes place at the establishment of the employment legal status. Data provided by the subjects as listed in Nftv Annex 3. I/A. shall be registered.
(5) The registry is operated in mixed system, on computers and manually. The controller is responsible for data security. In establishing digital data security, the IT Department shall support the records operator.
(6) From the employment records data service is available within the University for the rector, the chancellor, the department of wages and labour, the head of the unit with competence in economic affairs as well as the heads and staff competent in personnel and economic affairs of units where the subject performs their task.
(7) For the security of data stored on the servers of the IT Department operating the IT system shall take measures and maintain a high standard as laid down in 11.§ Subsection (9) of this regulation.
(8)The data controller is the Department of Wages and Labour of the Directorate of Economic and Technical Management and the competent staff of administrative units. The rights of access are allocated by the Department of Wages and Labour to make sure the controllers can process and read only data of their scope of competence.
(9) Employee data are processed
a) by the DSA in the context of and to an extent necessary for the operation and use of the HR module of Neptun,
b) the Tenders Office in the context of and to an extent necessary for the operation and use of the Electronic Tendering System of the University (EPER),
d) the University Library with regards to data to upload to the Hungarian National Scientific Bibliography (MTMT) and the use of the library system.

21.§ Wages and Labour records

(1) In the wages and labour records, provisions referring to the employment register shall govern with differences described in this section.
(2) The controller of the wages and labour records is the Department of Wages and Labour – to an extent necessary for the fulfilment of their scope of tasks – authorised staff of administrative units and the Hungarian Treasury with regards to the centralised salary payroll.
(3) The records shall be managed on computrers.

22. § Other IT services

(1) For the operation of its IT services and especially the mail and library systems, the University provides central access services.
(2) In order to implement the provisions of Subsection (1), the IT Department operates an access control system supporting the University IT services using personal data from the employment registry and the Neptun.
(3) In the context of the provisions of Subsection (1), data of individuals not holding a legal relationship with the University described in Section 1. but using the University Library system shall be processed by the University Library with regards to the use and to an extent necessary for the Library system.
(4) The rules of operation of the MTMT database is contained by a special regulation of the University.

23.§ Electronic check-in system

(1) Where there is an electronic check-in system at the University, its purpose is the recording of the time of employees' arrival at and departure from their workplace.
(2) The electronic check-in system installed in the University is used with a card allowing permanent access.
(3) The following range of staff is entitled to a permanent check-in card:
a) individuals holding public employment, work contract or other work-related legal status with the University who work in the given building;
b) individuals employed by other organisations connected to the operation of the University who work in the given building.
(4) The administrational unit of the University involved shall keep a record of the permanent access cards (card records) which shall contain:
a) card number,
b) user's name,
c) user's ID (ID may be suitable to individual identification only – but different from University IDs used for other purposes),
d) duration of validity (indefinite or definite period),
e) the definition of the territory affected by the right of access.
(5) Access to the data of card registry is available only for staff appointed by the head of the administrative unit in question and authorised for such data processing by their scope of work. Inspection into data registry is allowed in special cases: suspicion of administrative or criminal offence. Inspection is granted by the head of the administrative unit in question.
(6) Data related to permanent access cards are erased on termination of the user's legal status allowing permanent access, within 30 days from surrendering the card but for the day of legal status retrospectively.

24.§ Electronic surveillance system

(1) Where electronic surveillance system is installed at the University, its purpose is the prevention of unauthorised entry into the premises and resulting possible crimes against property.
(2) In the course of operating the electronic surveillance system video recordings containing personal data are made.
(3) In the course of positioning the cameras, it must be taken into consideration that the surveillance system shall not violate human dignity, the cameras shall not monitor employees' private lives and that the viewing angle of the cameras may be set only on territories in accordance with their purpose.

(4) The University – pursuant to Mt. 11. § (2) and Infotv. 20. § (2) – shall ensure that visitors to the University premises receive prior information with details prescribed by law about the significant requirements of data processing related to the electronic surveillance system.
(5) The information for employees and students is the responsibility of the administrative unit operating the electronic surveillance system. The leaflet shall mention in relation to every camera, for what purpose it was positioned in that location and which territory its viewing angle covers. The leaflet described in Subsection (4) shall be made available for new employees on entry, for students on registry. A copy of the leaflet shall be attached to the employee's – signature needed – and the student's personal file.
(6) Pursuant to Act CXXXIII of 2005 on persons and property protection and on the activity of private detectives 28. § (2) item c), for third parties wishing to enter its premises, the University shall position signs at monitored spots to raise awareness of the surveillance system operating.
(7) The cameras record only images. The CCTV system applied by the university can be used for direct observation (live image); only staff of the reception service have right to indirect observation and only to the extent necessary for the performance of their duties. The display for viewing and possible reviewing of the image files must be positioned in a way that individuals outside the scope of eligibility cannot see them while the images are viewed.
(8) The cameras record images 24 hours a day. The records are stored on a hard disk for 3 working days, after which the system automatically overwrites the files rendering them unrecoverable.
(9) The reviewing of the images is possible in special cases. Only the head of the body operating in the premises (rector and chancellor), individuals appointed by them, or bodies empowered by legislation hold authority. Special cases include the suspicion of disciplinary offences, administrative or criminal offences. The files shall be transferred by the University only on direct request of jurisdiction or authority. The reviewing, data transfer and possible saving shall be documented.

25.§ Access to and dissemination of public data

(1) Data whose dissemination is mandatory (pursuant to Infotv Annex 1.) is made available by the University on its homepage for anyone without personal identification, unlimited, printable and copiable, free of charge for the purposes of inspection, download, printing, copying, network data transfer. The updating of the data at specified intervals is initiated by the data officer. The disseminated data shall be protected from unauthorised alteration, erasure, destruction and damage.
(2) The University allows free access to the public data and data accessible on public interest grounds in its control – with the differences defined in Infotv. – on direct request for anyone. The application may be submitted verbally, in writing or digitally (Annex 4. a). Verbal applications must be recorded in written form according to Annex 4. a) not later than two working days from the arrival of the verbal application. The date of arrival of the verbal application is the day of its recording in written form.
Unless provided otherwise by statutory law, the personal data of the data applicant may be processed to the extent necessary for paying the fee charged for meeting the demand and preparing copies. Immediately after the lapse of time defined by Infotv. and the payment of the costs, the personal data of the applicant must be erased.
(3) Data of an individual acting in the competence of the University accessible on public interest grounds are their name, task, position, executive capacity, other personal data in the context of their public duties and other personal data rendered public by law. Data accessible on public interest grounds may be disseminated by observing the principle of purpose limitation of data processing. For the dissemination of data accessible on public interest grounds Annex 6. and

the separate act of law on the publication of data accessible on public interest grounds on homepages shall govern.
Unless otherwise provided by law, data accessible on public interest grounds qualify as data controlled by bodies or individuals providing services which are either mandatory based on contracts concluded with national or local government agents or are impossible to meet otherwise, refer to these activities and are not considered public.
(4) Data of public interest or data accessible on public interest grounds are not accessible if they fall under the act on the protection of classified information.
(5) Data generated or recorded in the course of a decision making procedure within the competence of the University, serving to support the decision shall not be public for ten years from generation. Access to this data – by assessing the gravity of public interest in accessing vs. blocking accessibility of the data – can be granted by the controlling administrative unit or the head of the body in question.
(6) If the application for data is not clear, the controller shall call the applicant to clarify the demand. If the applicant fails to respond to the call for clarification, the application shall be considered as withdrawn. The applicant shall be notified of this fact.
(7) The controller shall grant the application for access to data of public interest in the shortest possible time but not later than fifteen days following the arrival of the application.
(8) If the application refers to data substantial in volume or in number, the deadline specified in Subsection (4) may be extended once fifteen days. The University data protection officer shall notify the applicant of this within fifteen days of delivery of the application.
(9) The delivered application for data of public interest shall be forwarded by the controller to the University data protection officer within two days. If the application did not arrive at the administrative unit entitled to data service, the officer shall, assessing the subject of the application, immediately (not later than 3 days) appoint the unit obliged to perform the data service and competent in compiling the reply, then forward the appointment with the application for data of public interest to the head of the unit.
If the demand can be met, the administrative unit appointed to data service shall prepare the data – or, on the applicant's request – the copies made of them for inspection or sending, and send their proposal – containing the calculation of a possible fee and its amount – through the officer to the chancellor for decision making. The University data protection officer shall keep a data of public interest service registry based on the information received from the unit meeting the demand (Annex 4.).
(10) The applicant may receive a copy of the document or part of document containing the data. The controller may– by authorisation of Govt. Decree 301/2016 (IX.30.) – charge a fee for making a copy, of the amount of which the applicant shall be notified by the University data protection officer before satisfying the demand. The applicant shall declare whether they maintain their order within thirty days from the delivery of the received information. The period from sending the notification until the applicant's declaration arrives at the University is not calculated into the deadline available for satisfying the data application. If the applicant maintains their order, they shall pay the fee to the University within a deadline of at least fifteen days.
On establishing the amount of the fee the following cost elements are to be taken into consideration: the cost of the medium containing the ordered data, the cost of delivery of the medium containing the ordered data to the applicant, also, if satisfying the order of data leads to the disproportionate use of the labour resources necessary for the performance of the core activities of the public body, the charge of workforce-input needed for satisfying the data order. The calculable amount of cost elements is defined by law.
(11) If the document containing data of public interest also contains data restricted for the applicant, the restricted data shall be rendered unrecognizable on the copy.

(12) Data requests shall be complied with in an easily recognisable form and - if the controller can perform this without disproportionate difficulties – with the technology and method required by the applicant. If the ordered data were disseminated in electronic form earlier, the request may be satisfied by marking the public source containing the data.
(13) Of the refusal of the application, reasons for the refusal and information on remedies the applicant is entitled to pursuant to Infotv., the University data protection officer shall, after negotiation with the appointed administrational unit, notify the applicant within fifteen days from the delivery of the order in written form – or if the applicant sent their e-mail address in the order – in e-mail. The officer shall keep a record of rejected applications and the reasons for rejection (Annex 4.).
The University is not obliged to comply with data requests in parts where requests for identical data range were applied for by the same applicant within a year unless the data belonging to identical range were modified; or if the applicant does not give their name, in case of non-natural entity their designation or the contact details where any information concerning the data request could be sent.
Information about possibilities of legal remedy shall contain that in the event of the violation of their rights, the applicant may turn to the University data protection officer with complaint (the complaint shall be investigated pursuant to 13. § (14) of this regulation, or the applicant may initiate an investigation at the Authority with reference to the fact that the applicant suffered impairment of right with respect to exercising their right of access to data of public interest, or there is a direct threat thereof, or in the event of rejection of the application, the applicant may turn to the competent court of justice within 30 days from delivery of the rejection. If, due to the rejection of the request, the applicant makes a report to the Authority in order to initiate an investigation, the action on the rejection of substantive examination of the report and the termination of the investigation shall be brought before the court in compliance with Infotv. 55. § (1) item b) on termination or within 30 days from the delivery of the notification pursuant to 58. § (3).
(14) If the request refers to data generated by any board or member state of the EU, the controller shall immediately take up contact with the EU board or member state involved and the data protection officer shall notify the applicant of this fact. The period from the notification until the delivery of the reply of the EU board or member state involved to the controller shall not be calculated into the deadline available for the compliance with the data request.
(15) If with respect to the rejection of application for access to data of public interest, legislation allows the controller discretion, the basis of rejection shall be given a narrow interpretation, and the demand for access to data of public interest may be rejected only if the public interest supporting the rejection weighs more than the public interest supporting compliance with the demand to access data of public interest.
Application for access to data of public interest may not be rejected on the grounds that a non-Hungarian speaking applicant drafts their application in their native tongue or any other language that they understand.
(16) In the event of the rejection of their application for access to data of public interest, or the expiry of deadline available for compliance or ineffective expiry of the extended deadline, also in order to ensure an effective review of the amount of fee charged for the compliance with the data request, the applicant may apply to any court of justice.
(17) The lawfulness of and grounds for rejection, also the merits of the amount of fee charged for making copies shall be proved by the University.

26. §

(1) Regarding the disclosure, rectification, updating or removal of data, the operator of the official University webpage shall log the date and time of occurrence of the event and the name of the user that contributed to the generation of the event.
(2) Data of public interest to be disclosed shall be sent by data sources – named in Annex 6. of this regulation - by e-mail to the appointed staff of the PR team of the Services and IT Directorate (hereinafter: data disseminator). The data source shall check the identicalness of the delivered and uploaded data. The data source shall continuously monitor the accuracy, timeliness and accountability of the uploaded public data after publication. The data source shall generate the rectified or updated data of public interest and forwards them to the data disseminator for the purpose of disclosure.
(3) The data disseminator shall check the data of public interest forwarded for the purpose of disclosure whether they comply with the conditions of publication format. The disseminator is responsible for the electronic publication, permanent accessibility, authenticity and updating of the forwarded data. Besides the new state of the updated data, the fact and time of update and the accessibility of the previous state in the archive files shall be indicated.
(4) The uploaded data – unless the Infotv. or other legislation provide otherwise – may not be removed from the homepage. In the event of the termination of the body, the obligation of publication falls on the legal successor.

27.§

(1) Any request from the media – anonymised pursuant to legislation – shall in all cases immediately be sent to the University data protection officer and the University spokesperson to prepare decision. The decision shall be made by the rector and the chancellor.
(2) If the applicant wishes to access the data after inspection, or to receive the copies personally, the data protection officer shall take up contact with the administration unit participating in satisfying the order and the applicant for the purpose of making an appointment. The requested data shall be presented to the applicant by staff of the unit participating in satisfying the order in the premises of the unit. By signing the declaration specified in Annex 4. b)-c) of this regulation – constituting part of the file – the applicant shall acknowledge that they have been granted inspection into the documents and that they have received the copies. In the event of the failure of submitting such a declaration, the applicant shall not be allowed access to the documents.
Appropriate time shall be granted for studying the data in the room specially designated for this purpose. While the applicant studies the presented document careful attention shall be paid to answering the applicant's questions, the security and unchanged state of the data. The applicant is entitled to take notes of the presented documents. The applicant may receive copies of the document or part of document containing the requested data disregarding the method of storage, against reimbursement.
(3) The data disclosure obligation laid down in this section shall be satisfied by the public institute of education maintained by the University, on its own homepage. Disclosure shall be ensured by the head of the institute of public education.

28.§ Closing provisions

(1) This regulation was adopted by the Senate of Kaposvár University by electronic vote on 25 May 2018. in Decision No. 43/2018. (V. 25.). The regulation enters into force on the day of its adoption, while the previous Security Policy of Kaposvár University as well as the Rector's Orders No. 2. and 3. of 2013. shall terminate simultaneously.
(2) The University shall comply with its information obligation concerning the rules of individual application for data of public interest by uploading this regulation on its internet homepage.

(3) In questions not regulated in this document the regulations of IT security, record management and other regulations of the University, relevant current Hungarian legislation and EU Decree No. 2016/679 shall govern.

Kaposvár, 25 May 2018.

Prof. Dr. Szávai Ferenc DSc	Dr. Borbás Zoltán
rector	chancellor

Annex 1

Data breach record of Kaposvár University

The University data protection officer shall keep records to control data breach related measures and to notify the data subject.

No.	The scope of personal data involved	The range of entities involved in the data breach	Number of entities involved in the data breach	Date and time of the data breach	The circumstances of the data breach	The effects of the data breach	Measures taken to eliminate the data breach	Other data specified by legislation prescribing data processing	Date of entry

Annex 1. a)

Content of data breach report

Content of report sent to *The Authority*:

a) the nature of the data breach including – if possible – the range and number of involved entities, the scope and estimated quantity of data involved in the data breach,

b) provides information on the name and contact details of the data protection officer or other official appointed to provide further information,

c) presents the possible consequences of the data breach, and

d) presents the measures to handle the data breach – aimed at the mitigation of potential adverse consequences and others – taken or planned by the University.

The notification of the data subject shall contain the description of the nature of the data breach, and suggestions aimed at the mitigation of potential adverse consequences for natural entities.

On establishing the detailed rules referring to the form of the notification about the data breach and the procedures to be applied, the circumstances of the data breach shall receive extra attention including the fact whether the personal data were protected with adequate technical protective measures which efficiently restrict the probability of occurrence of abuse with personal data or other forms of abuse. These rules and procedures shall also take legitimate interests of the law enforcement authorities into consideration in cases when early disclosure would unnecessarily risk the investigation of the circumstances of the data breach.

Annex 2

Data transmission records of Kaposvár University

The controller shall, through the territorial data protection officer, for the purpose of examining the lawfulness of the data transfer and the notification of the data subject, keep records of data transmission, which – unless legislation or university regulation establishes a longer period of time – shall be stored for 5 years, in case of special data for 20 years.

No.	The name of the administrational unit satisfying the data service (controller)	Time/frequency/ method of transferring personal data	Legal basis of data transmission	Recipient of data transmission	Definition of scope of transferred personal data	Range of data subjects	Other data specified in legislation prescribing data processing (name and address of requesting body/individual; purpose/legal grounds/time of data request)	Security measures taken in the course of data transmission	Name of registrar, date of entry

Annex 2. a.)

Data transmission application form – Based on student data registry

Name, mail address and phone number of body or individual initiating data service	
Objective and intended purpose of data request	
Legitimate grounds for data request or the declaration of the data subjects	
Date and time of data request	
Deadline of data service	
Frequency of data service (regular or single demand)	
Range of data subjects	
Scope of requested data	
Method of data transmission	

Annex 3.

Data processing records of Kaposvár University

All data processing performed at the University shall be recorded. Registration shall be initiated by the controller with the University data protection officer (name and contact details) before commencing data processing.

name and contact details of staff logging data processing	data processing administrational unit, name and range of controllers	Name and position of individuals with right to access	purposes of data procession	legal ground for data procession	range of data subjects (and number if known)	scope and source of data	data transmission: range of recipients (in case of third country recipients/international bodies guarantees of conformity), frequency, legal ground	deadline of erasure of data categories	general description of technical and administrative measures (pursuant to GDPR regulation 32. (1))

Annex 4.

Record of transferring data of public interest at Kaposvár University

No.	Sender (without ID)	Date of delivery to the University	Date of delivery to the data protection officer	Requested data of public interest	Name of administrative unit involved	Data of public interest released (dd_mm_yy_) / name of operator/ method of release	Reply: ab ovo uploaded on the University homepage (dd_mm_yy_) / method	Application for access to data of public interest rejected (dd_mm_yy_) / grounds	Extension of deadline (last day of extended deadline of procedure)	Contains data for the preparation of decision, notification of applicant of this fact	Contains data for the preparation of decision, proposal for decision	Relocated in the absence of competence (dd_mm_yy_, where_)	Legal remedy action initiated	Decision made in legal remedy action

Annex 4. a)

Application [*]

for access to data of public interest

Name of applicant (name of individual, designation of legal entity or other body without legal personality):	
Name of representative (acting representative in case of legal entity or other body without legal personality):	
Mailing address:	
Daytime contact details (telephone, fax, e-mail address):	
Definition of requested data of public interest:	
Copies of the data requested (underline where applicable):	yes no
Fill in only in case of request for copies! I want to receive the copies (underline where applicable):	in person by mail by e-mail

I undertake to pay the costs incurred by producing copies to Kaposvár University prior to receiving the copies.

By giving my signature I acknowledge that if the application I submitted for access to data of public interest needs rectification or completion in order to ensure it can be satisfied, and I fail to provide necessary information to the controller's request, the controller shall consider my application withdrawn.

Issued: …….

……

signature

[*] After the termination of the case the personal data shall be erased pursuant to 25.§ (2) of this regulation.

Annex 4. b)

Declaration on inspection into records

I, undersigned (name of applicant[†]) …….. wish to make this declaration:

1. On this day I had inspection into the records listed below (title of inspected material), of which I require/do not require copies:
   ……..……..……..
   ……..……..……..……
   ……..……..……..……
   ……..……..……..
2. I shall use and process the data accessed in the course of inspection pursuant to Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information with attention to provisions of Hungarian legislation concerning rights of personality and the protection of intellectual products.

Issued: …….

……

signature

Annex 4. c)

Declaration on personal reception of requested copies

I, undersigned (name of applicant[‡]) …….. wish to make this declaration:

On this day I received copies of the records listed below (title of inspected material).

……..……..……..
……..……..……..……
……..……..……..……
……..……..……..

Issued: …….

……

signature

[†] After the termination of the case the personal data shall be erased pursuant to 25.§ (2) of this regulation.
[‡] After the termination of the case the personal data shall be erased pursuant to 25.§ (2) of this regulation.

Annex 5.

Records of interconnection of data processing

No.	Designation of interconnected data processing operations	Objective, and intended purpose of interconnection	time and duration of interconnection	legal grounds (statutory law, university regulation)	name, administrative unit, contact details of staff performing interconnection	entities involved with the interconnection and their number	scope of interconnected data	method of interconnection (manual, computer, mixed)	data security measures

The first copy stays with the administrative unit performing the interconnection, a second one shall be forwarded to the University data protection officer. The records shall be stored at the controller for ten years, then be deposited in the archive.

Annex 6. a)

GENERAL DISSEMINATION LIST

I. Administrative, personnel data

	Data concerning the public body	Update	Retention	Data source
1.	Official name, headquarters, mailing address, telephone and fax number, e-mail address, homepage, contact details of customer service	Immediately after the changes	Delete previous status	vice rector for strategy and development of education
2.	Administrative structure with the denominations of units; responsibilities of individual units	Immediately after the changes	Delete previous status	director of services, heads of administrative units
3.	Names, positions, contact details (phone/fax/e-mail) of management and heads of individual units	Immediately after the changes	Delete previous status	chancellor
4.	In case of collegiate body, the numbers, composition, members' names, position and contact details	Immediately after the changes	Delete previous status	head of involved body
5.	Designation and data listed in (1.) of other public bodies operating under its management, supervision, or in its subordination	Immediately after the changes	With keeping the prior status in archive for 1 year	vice rector for strategy and development of education
6.	Name, headquarters, contact details (phone/fax/e-mail), scope of activity, name of representative of business entity in its majority ownership or operating with its participation; public body's level or shareholding	Immediately after the changes	With keeping the prior status in archive for 1 year	asset management officer
7.	Name, headquarters of budgetary entity established; designation of the legislation founding the entity, its founding decision, articles of association, CEO, webpage, operating licence	Immediately after the changes	With keeping the prior status in archive for 1 year	director of services, heads of administrative units
8.	Titles of papers founded, name and address of editorial and publisher; name of editor-in-chief	Immediately after the changes	With keeping the prior status in archive for 1 year	rector / heads of faculties involved
9.	Data specified in (1) of higher authority or supervisory body, regarding its official decisions, of the body entitled to assess the appeal, in the absence thereof the body exercising legal control	Immediately after the changes	With keeping the prior status in archive for 1 year	rector, chancellor

II. Data concerning activity, operation

	Data concerning public body	Update	Retention	Data source
1.	The valid and full text of related basic legislation, legal instruments of state administration defining its scope and core activities, as well as the organisational and operational regulation or order of business, and the data protection and data security regulation	Immediately after the changes	With keeping the prior status in archive for 1 year	rector, chancellor
2.	Designation and content of public services provided by or financed from its budget; the order of access to the services, the amount of fee charged for the services, discounts from the fee	Immediately after the changes	With keeping the prior status in archive for 1 year	administrative unit involved and CFO / vice-director
3.	Descriptive data of databases or records maintained (name, format, purpose and legal grounds of data processing, range of subjects, sources of data, in case of a questionnaire data collection, the questionnaire to be completed), the identification data of records to be reported to the data protection records in compliance with this law; types of data collected and processed in the framework of its core activity, the method of access, the costs of making copies	Immediately after the changes	With keeping the prior status in archive for 1 year	head of administrational unit appointed for the management of database/registry, collection and processing of data
4.	Title, topic of publicly available publications, way of access, no-charge nature or amount of remuneration	Quarterly	With keeping the prior status in archive for 1 year	head of unit appointed for editing publications
5.	Collegiate body: order of preparation of decisions, methods of citizens' contribution (commenting), rules of procedures; place, time and publicity, decisions, records and summaries of meetings; data of votes unless restricted by law	Immediately after the changes	With keeping the prior status in archive for 1 year	head of body involved
6.	Public body: communications and notices published	Continuously	With keeping the prior status in archive for 1 year	rector / chancellor / in other cases the head of the unit publishing the communications and notices
7.	Professional description, results and reasons of tenders launched	Continuously	With keeping the prior status in archive for 1 year	head of the unit responsible for announcing and management of tenders
8.	Public findings of examinations and testing performed at body	Immediately after access to the report on examination	With keeping the prior status in archive for 1 year	rector, chancellor
9.	Order of arrangement of applications for access to data of public interest, name, contact details and place of appointment of competent administrational unit; name of data protection officer or staff responsible for information rights	Quarterly	Delete prior status	chancellor, head of unit involved

10.	Results of law-based statistical data collection concerning activity, their evolution over time	Quarterly	With keeping the prior status in archive for 1 year	CFO / vice director, vice rector for strategy and development of education
11.	Relevant data of obligatory statistical reporting regarding data of public interest	Quarterly	With keeping the prior status in archive for 1 year	manager responsible for data reporting
12.	Special and individual disclosure list	Immediately after the changes	Delete prior status	rector, chancellor

III. Business data

	Data concerning public body	Update	Retention	
l.	Annual budget, report according to the Accounting Law or annual budget report	Immediately after the changes	For ten years after publication	CFO / vice director
2.	Aggregate data concerning the number and staff expenditure; also the aggregate amount of the salary, wages and other regular bonuses and allowances as well as the aggregate amount and types of expenditure for other staff	Quarterly	Keep in archive for the period specified in legislation but at least one year	Head of Dept. of Labour
3.	Data concerning the names of beneficiaries of budget support provided in compliance with the Public Finances Act, the purpose, amount and place of implementation, unless the support is withdrawn or the beneficiary resigns before implementation	For sixty days from making the decision	For five years after publication	CFO / vice director
4.	Designation (type), subject of contracts related to the use of government funds, the management of government-operated assets, the order of public supplies, construction work investment, services, sale of business, asset recovery, transfer of property or property value rights as well as awarding concessions, the names of contracting parties, the value of contracts, in case of contracts concluded for a definite period, its period, as well as the modification of such data, except the data of procurement in the field of defence and security and classified data, also procurements pursuant to Act CXLIII of 2015 9. § (1) *b)* on public procurement and contracts concluded as a result thereof. Contract value shall mean the consideration stipulated for the subject matter of the contract calculated without VAT. In the event of a free transaction, the higher amount of the market value and the book value shall be taken into consideration. For periodically returning contracts – concluded for periods over a year – the amount of consideration calculated for one year shall be	For sixty days from making the decision	For five years after publication	CFO / vice director

	used as a basis. The value of contracts concluded with the same subject matter with the same party in the same year shall be calculated in one aggregate sum.			
5.	Payments exceeding five million HUF made for other than the performance of core activities (especially sponsoring clubs, professional and employee advocacy bodies, organisations supporting education, cultural, social and sport activities for employees and beneficiaries, payments in connection with tasks performed by foundations)	Quarterly	Keep in archive for the period specified in legislation but at least one year	CFO / vice director
6.	Description of development projects implemented with EU support, contracts involved	Quarterly	Keep in archive for at least one year	CFO / vice director, Head of Tenders Office
7.	Public procurement information (annual plan, summary on the evaluation of tenders, contracts concluded)	Quarterly	Keep in archive for at least one year	CFO / vice director, Head of Tenders Office

Annex 6. b)

SPECIAL DISSEMINATION LIST

I. Organisational, personnel data

	Data	Update / legislation prescribing publication	Retention	Data source
1.	University Organisational and operational regulation	Immediately after the change / Nftv.	Do not delete the previous state.	Secretary of the Senate

II. Data on activity and operation

	Data	Update	Retention	Data source
1.	Composition and decisions of the Senate	pursuant to SZMSZ / Nftv.	Do not delete the previous state.	Secretary of the Senate
2.	The results of graduate tracking survey in the form of abridged summary and full study	At least annually / Vhr.	Do not delete the previous state.	head of the administrational unit performing the survey
3.	Institutional information	At least every six months / Vhr.	Do not delete the previous state.	Director of Academic Affairs

III. Business data

	Data	Update	Retention	
1.	Data specified in 43.§ of Act CXLIII of 2015. on Public procurement (Kbt.)	Immediately after the change / Kbt.	As specified in Kbt	CFO / vice director
2.	The performance of net HUF 100 million as a result of public procurement procedure (from institutional appropriations)	Within 8 days of payment / 368/2011. (XII.31.) Govt. Decree on the implementation of the Public Finances Act	Do not delete the previous state	CFO / vice director, Head of Tenders Office

Annex 6. c)

CUSTOM DISSEMINATION LIST

I. Organisational, personnel data

	Data	Update	Retention	Data source
1.	Articles of Association, Operating Licence of the University	Immediately after publication in official gazette	Keep in archive for 5 years after publication.	rector, chancellor
2.	The regulations of the University	Immediately after the changes	Do not delete the previous state.	head of administrational unit involved

Annex 7.

DATA PROCESSING INFORMATION[4]
for individuals entering into public employment, work contract or any work-related legal relationship with the University

Kaposvár University as employer/principal, is entitled and liable to keep records of the data specified in Annex 3. I/A, Act CCIV of 2011. on National Higher Education, which, as provided in Subsection 4. of the above mentioned part of legislation, it may forward.

The designation of the employer, the name and position of the public employee are data of public interest, which may be disclosed without the public employee's prior knowledge and consent.

I acknowledge that

- the staff and the management of Kaposvár University may have access to and process my personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.
- if, responding to an external invitation, I submit a tender through the University, the submission of my application shall be considered as my unambiguous consent that the University of Kaposvár may transfer my tender-related personal data to the principal and the body entitled to examine the submission, implementation and the accounts of the tender.

The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation fo Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

Issued: …….

……
signature

[4] In case of public employment status, the information shall be provided in soft or hard copy; in case of work contract or other work-related legal status, the information shall be built in the text of the contract.

Annex 8.

DECLARATION AND INFORMATION FOR DATA PROCESSING[5]
for individuals entering into student status or doctoral student status with the University

Undersigned: ……(name) ……((place and date of birth) …… (mother's name) acknowledge that

- Kaposvár University as employer/principal, is entitled and liable to keep records of the data specified in Annex 3. I/A, Act CCIV of 2011. on National Higher Education, which, as provided in Subsection 4. of the above mentioned part of legislation, it may forward;
- The staff and management of Kaposvár University, the University Student Union and its divisions, the University Doctoral Student Union and the representatives of the faculty doctoral student agencies in the context and to the extent of the performance of their official job duties and their managerial assignments may have access to and process my personal data.

The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

By signing this declaration, I give my consent, that my personal data processed in the record of Kaposvár University – over cases laid down in Annex 3. I/B, Subsection 4. Act CCIV of 2011. on National Higher Education – to the extent necessary for achieving the goal specified in the request, may be allowed access to the range I specify below (check where appropriate):

work providers
members of the University alumni system
for research, opinion survey.

I give my consent that, after the termination of my student status, the University contact me for the purpose of the quality assurance of the programme.
I acknowledge that teachers and students may use my personal data in the Neptun electronic education system with the help of the suitable search function to find the name I bear and my Neptun ID code as well as send messages to me.
I acknowledge that it is considered as my unambiguous consent to data transfer as described above if I make the appropriate declaration on the personal, password-protected portal in the electronic education system.
I acknowledge that if, responding to an external invitation, I submit a tender through the University, the submission of my application shall be considered as my unambiguous consent that the University of Kaposvár may transfer my tender-related personal data to the principal and the body entitled to examine the submission, implementation and the accounts of the tender.
I acknowledge that if I am awarded a scholarship defined by the university regulation or the statutes of the University Student Union (local unions included) and the University Doctoral Student Union (faculty agencies included) as such – pursuant to provisions of the regulations of Kaposvár University – the fact thereof and the goal of the tender and the amount funded may be disclosed.

Issued: ……

……...
student

By witness whereof:

Name: .....
Address: .....
Signature: .....

Name: .....
Address: .....
Signature: .....

[5] Information shall be sent in a personal notification through the Electronic Education System.

Annex 9.

INFORMATION ON DATA PROCESSING[6]
for individuals applying for admission at the University in the context of higher education admissions information

Kaposvár University as employer/principal, is entitled and liable to keep records of the data specified in Annex 3. I/A, Act CCIV of 2011. on National Higher Education, which, as provided in Subsection 4. of the above mentioned part of legislation, it may forward.

The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.

The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

[6] The information shall be published in the higher education admissions brochure.

Annex 10.

Information on data processing[7]
for individuals applying for jobs at the University included in the call for job tenders

Kaposvár University, as advertiser of job applications shall, as provided in 18. § (1) d) of Act CCIV of 2011. on National Higher Education, process personal data submitted in context of job application until the evaluation of the tender.

The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.

The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

[7] The information shall be published with reference to the url as in Subsection 3. of the call for job tenders on the University homepage, by the accurate indication of the path.

Annex 11.

Information on data processing[8]

I. Information provided for participants of adult education programmes organised and run by the University

Pursuant to 21. § (1) of Act LXXVII of 2013. on adult education, in order to implement the adult education programme/course (hereinafter: training) selected and to be heard by you, Kaposvár University shall process your data (the details of the scope of data is available in the regulation and information brochure mentioned below), for which you have given your consent by signing the training agreement.
The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.
The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

II. Information for individuals not in legal relationship with the University, applying for habilitation procedure or participating in such

Pursuant to 6. § (4) of Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information, in order to implement the habilitation procedure initiated and taken by you shall process your data (the details of the scope of data is available in the regulation and information brochure mentioned below), for which you have given your consent by signing the application for launching the habilitation procedure.
The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.
The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

III. Information provided for individuals not in legal relationship with the University, applying for doctoral degree obtainment procedure and participating in such

Pursuant to 6. § (4) of Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information, in order to implement the doctoral degree obtainment procedure initiated and taken by you shall process your data (the details of the scope of data is available in the regulation and information brochure mentioned below), for which you have given your consent by signing the application for launching the doctoral degree obtainment procedure.
The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.
The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data

[8] The information shall be built in the text of the application for adult education programme, the application for launching the habilitation procedure, the application for doctoral degree obtainment procedure and the registration necessary for the use of library service.

Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

IV. Information for individuals not in legal relationship with the University, using the library system of the University

Pursuant to 57. § (1) of Act CXL of 1997 on the protection of cultural goods, museum institutions, public library services and community culture and 6. § (4) of Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information, Kaposvár University, in order to provide you with the library service taken by you shall process your data (the details of the scope of data is available in the regulation and information brochure mentioned below), for which you have given your consent by signing the registration necessary for using the service.

The staff and the management of Kaposvár University may have access to and process your personal data in the context of and to the extent necessary for performing their job duties and their managerial assignment.

The rules of processing and protection of personal data are contained in Act CXII of 2011. on the Right of Informational Self-Determination and on Freedom of Information and the Data Protection Regulation of Kaposvár University, which is available on www.ke.hu in the Data of public interest and Data protection menu options.

Annex 12.

Information on the operation of electronic access control system and electronic surveillance system in the premises of Kaposvár University_____ /name of administrational unit/[9]

a) legal grounds for data processing:
The Data Protection Regulation of Kaposvár University. Downloadable from:
_____

b) Description of the positioning of individual cameras, their purpose, the territory or object observed, whether the camera in question performs direct or fixed observation.

_____

c) Operator of CCTV system:

_____

d) Place and duration of storing the files:

_____

e) Data security measures concerning the storing of the data:
The Data Protection Regulation of Kaposvár University. Downloadable from:_____

f) Range of individuals with right to access data, definition of individuals or bodies to forward data to and in what cases:
_____
_____
_____

g) Rules concerning reviewing the files, purposes to use the files for:
_____
_____
_____

h) Rights of employees with respect to the CCTV system and methods of exercising them:
The Data Protection Regulation of Kaposvár University. Downloadable from: _____

i) Legal remedies available in case of violation of the right to informational self-determination:
The Data Protection Regulation of Kaposvár University. Downloadable from: _____

……., „……..(nap)” „…….” (month) 20…..

In the event of entering into work-related legal status with the University:
I acknowledge the information above.

Name (block capitals): _____ _____
(legible signature)/

[9] For individuals using the University infrastructure, the information shall be provided in writing.

Annex 13.

DECLARATION OF CONFIDENTIALITY

in case of public employees or work-related contracts

Undersigned, …….. (name of employee) …….. (place and time of birth) …….. (mother's name) …….. (permanent address) …….. (position) …….. (administrative unit)

as one in public employment or other work-related contract with Kaposvár University (hereinafter: University) I commit to retain any personal data, classified data I have access to as a result of the activities of the institute and performing my job duty, or fulfilling my tasks, and also data qualifying as data protected by legislation or limited to the practising of a profession and every fact or circumstance the disclosure of which may have adverse consequences to the University, any of its employees, students or contractors, or otherwise would create an unlawful situation. I also undertake not to provide unauthorised individuals with information about the mentioned data, not to publish or disclose them unlawfully.

The secrecy does not extend to the publicity of data of public interest or the data service and information obligation specified in legislation with regards to data public for public interest, also data that the subject gave prior consent to disclose, approved of their publication.

Furthermore, I declare that in the event I fail to comply with this declaration, I shall endure its adverse legal consequences.

Kaposvár, 20……

.....

employee

By witness whereof:

Name:	Name: .....
Address:	Address: .....
..... .	.....
Signature:	Signature: .....

Annex 14.

DECLARATION OF CONFIDENTIALITY

for contracting partners

Undersigned, …….. (name of employee) …….. (place and time of birth) …….. (mother's name) …….. (permanent address)

I commit to retain any personal data, classified data I have access to as a result of the activities of Kaposvár University (hereinafter: University) and performing my job duty, or fulfilling my tasks, and also data qualifying as data protected by legislation or limited to the practising of a profession and every fact or circumstance the disclosure of which may have adverse consequences to the University, any of its employees, students or contractors, or otherwise would create an unlawful situation. I also undertake not to provide unauthorised individuals with information about the mentioned data, not to publish or disclose them unlawfully.

The secrecy does not extend to the publicity of data of public interest or the data service and information obligation specified in legislation with regards to data public for public interest, also data that the subject gave prior consent to disclose, approved of their publication.

Furthermore, I declare that in the event I fail to comply with this declaration, I shall endure its adverse legal consequences.

Kaposvár, 20……

.....

declarant

By witness whereof:

Name:	Name: .....
Address:	Address: .....
..... .	.....
Signature:	Signature: .....

Annex 15

Complaints management records

No..	Name, address, phone number of complainant individual/body	Administrational unit / controller (recipients of complain)	Time of delivery/ Time of delivery at the University data protection officer (day, month, year)[10]	Deadline; in the event of extension the new deadline (day, month, day) / notification for the complainant[11]	Subject of complaint / scope of data involved	Name and contact details of administrational unit(s)/ controllers	Cooperator's task in procedure	Complainant's hearing (if necessary)[12]	Conclusion of investigation: informing the complainant		Date of entry
									on measures taken	on the rejection of the complaint, omitting measures (with reasons and possibilities of legal remedies)	

[10] Document containing transfer (e-mail, paper-based)
[11] Notification (e-mail, paper-based) for the complainant
[12] Record made on the hearing

Annex 16.

Attendance sheet

Data protection information / training

Venue:

Time:

Name and position of data protection instructor:

I, undersigned, declare that I took part in the Data protection training/information session at the time specified above. I got acquainted with the valid data protection regulation of Kaposvár University and I undertake to be bound by them:

No..	**Name, position**	**Administrational unit**	**Signature (legible)**