UNIVERSITY OF DUNAÚJVÁROS

DATA PROCESSING AND PRIVACY POLICY

Dunaújváros

2022

Adopted
by the Senate of the University Of Dunaújváros by Resolution 31-2021/2022.(22.03.2022)

Effective from: 23.03.2022

Amended and consolidated by the Senate of the University of Dunaújváros by Resolution 54-2021/2022 (17.05.2022)

Effective from: 18.05.2022

TABLE OF CONTENTS

PREAMBLE

On the basis of the following relevant legislation,

- Act CXII of 2011 on the Right of Informational Self-determination and Freedom of Information (hereinafter Infotv.);
- Act CCIV of 2011 on National Higher Education (hereinafter Nftv);
- Act I of 2012 on the Labour Code
- Act CXCV of 2011 on the Benefits of Persons with Disabled Work Ability and on the Amendment of Certain Acts;
- Act V of 2013 on the Civil Code
- Act CLII of 2007 on Certain Obligations to Declare Assets;
- Act CXXV of 1995 on National Security Services
- Act CXXXIII of 2005 on the Rules of Security Services and the Activities of Private Investigators;
- Government Decree 305/2005 (25 December) Korm. on the detailed rules concerning the electronic publication of data of public interest, the unified public data retrieval system, the data content of the central register and data integration;
- Recommendation of the National Authority for Data Protection and Freedom of Information (hereinafter Authority) on the basic requirements for electronic surveillance system in the workplace;
- Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation 95/46/EC (hereinafter Regulation),
- Government Decree 87/2015. (9 April) on the implementation of certain provisions of Act CCIV of 2011

the Senate of the University of Dunaújváros (hereinafter University) sets out this policy (hereinafter: Policy) as follows:

I. PART

GENERAL PROVISIONS

Section 1 Purpose and scope of the policy

(1) The purpose of this Policy is to define the legal order of operation of the records containing personal data kept at the University of Dunaújváros (hereinafter: University), to ensure the constitutional principles of privacy and the right of informational self-determination, and to ensure that within the limits of the law, everyone has access to their personal data and can access data of public interest, and to prevent unauthorised access, alteration or unauthorised disclosure of data.

(2) The purpose of the Policy is to ensure the exercise of the right of informational self-determination with respect to the protection of personal data, the rights to data protection and the requirements of data security in the activities of the University, to define the data protection and data security rules applicable to the processing of personal and sensitive data, to prevent unauthorised access, unauthorised alteration and disclosure of data, and to provide for the procedural rules to be followed in the event of a personal data breach, in order to prevent unauthorised use of personal data processed by the University.

(3) The purpose of the Policy is to facilitate the exercise of the constitutional right of access to data of public interest, taking into account the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information and other legislation, by defining the procedure for the disclosure of data, the procedure to be followed in the event of a request for access, the persons involved in the administration of the case, the persons responsible, the procedural rights and obligations of the person wishing to access the data and the University.

(4) Furthermore, the purpose of the Policy is to set out the procedure for the university's compliance with the obligation to publish data of public interest and public interest within its own organisation, as provided for in Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information and its implementation regulations.

(5) The scope of the Policy covers the processing of personal data, special data and data of public interest and public interest data carried out at the University by all its departments.

(6) The Privacy Notices for each department are issued in a separate document.

(7) The scope of the Policy also extends to bodies established by the University and which cannot be separated from the University in terms of IT system use within the University, as well as to any body or person who uses the IT infrastructure operated by the University (except for open access Internet use) or performs processing activities on the basis of the University's provisions or on behalf of the University.

(8) This Policy applies to processing and data handling performed by fully or partially automated means as well as to manual processing.

Section 2[1] Basic concepts and principles of privacy

(1) When applying this policy:

1. *data subject:* a natural person identified or identifiable from any information;

1a. *identifiable natural person:* a natural person who is identified or identifiable; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. *personal data:* any information relating to the data subject;

3. *special data:* any data that fall within special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons;

3a. *biometric data:* personal data relating to the physical, physiological or behavioural characteristics of a natural person obtained by means of specific technical procedures which allow or confirm the unique identification of the natural person, such as facial image or dactyloscopic data;

3b. *health data*: personal data relating to the physical or mental health of a natural person, including data relating to health services provided to a natural person which contain information about the health of the natural person;

4. *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;

5. *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;

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

7. *controller*: the natural or legal person or unincorporated organisation which, alone or jointly with others, determines the purposes for which the data are to be processed, takes and executes decisions regarding the processing (including the means used) or has them executed by a processor, within the limits set by law or by a legally binding act of the European Union;

1 From the relevant sections of the Regulation

8. *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, synchronizing or connecting, blocking, erasing and destroying 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);

9. *data transfer:* making data available to a specified third party;

9a. *indirect data transfer*: the transfer of personal data to a controller or processor in a third country or to a controller or processor in another third country or to a processor in an international organisation by transferring the personal data to the controller or processor in a third country or to a processor conducting processing in an international organisation;

9b. international organisation: an organisation governed by public international law and its subsidiary organs, and any other body which has been established by or under an agreement between two or more states;

10. *disclosure:* ensuring open access to the data to anyone;

11. *erasure of data:* the destruction or elimination of data sufficient to make them irretrievable;

12. *limitation of processing*: blocking of stored data by means of a flag to restrict further processing of the data;

13. *destruction of data:* the complete physical destruction of the medium containing data;

14. *processor*: a natural or legal person or an unincorporated organisation which processes personal data on behalf of or under the authority of the controller, within the limits and under the conditions laid down by law or by a legally binding act of the European Union;

15. *data source:* a body having public service functions, that is responsible for the inception - in the course of operations or otherwise - of any statutory public data to be published by way of electronic means;

16. *data disseminator:* a body having public service functions, that publishes data received from the data source on a website, unless it is published by the data source themselves;

17. *data set:* all data processed in a single register;

18. *third party:* any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

19. *personal data breach:* personal a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or transfer of, or access to, personal data transferred, stored or otherwise processed;

20. *profiling*: the processing of personal data by any automated means, which is intended to assess, analyse or predict the personal characteristics of the data subject, in particular their performance at work, economic situation, state of health, personal preferences or interests, reliability, behaviour, location or movements;

21. *recipient*: the natural or legal person or unincorporated organisation to whom or which personal data are disclosed by the controller or processor;

22. *pseudonymisation*: the processing of personal data in a way that makes it impossible to determine, without further information, to which data subject the personal data relate and to ensure, by technical and organisational measures, that the personal data cannot be linked to an identified or identifiable natural person.

23. *legitimate interest*: a legitimate interest of the controller, including the controller with whom the personal data may be shared, or of a third party, which may constitute a legal ground of processing, provided that the interests, fundamental rights and freedoms of the data subject do not override the legitimate interests of the data subject, taking into account the data subject's reasonable expectations on the basis of his or her relationship with the controller. The processing of personal data strictly necessary for the purpose of fraud prevention is considered to be in the legitimate interest of the controller concerned.

(2) Natural or artificial identifiers are used to identify the data subject. *Natural identification data* include, in particular, the name of the data subject, his or her mother's name, place and date of birth, address of residence or domicile. *Artificial identification data* means data generated by mathematical or other algorithms, in particular the personal identification code, the social security number ("TAJ"), the tax identification number, the number of the identity card, the passport number, the University student or lecturer identification number (NEPTUN code, Education ID).

(3) *Descriptive data* are other data relevant to the purpose of the processing. Descriptive data that cannot be linked to a specific natural person are not personal data (e.g. statistical data).

(4) Special data may be processed at the University within the scope, to the extent and for the duration regulated by the Act on Benefits for Persons with Disability. In addition, data relating to accidents at work, student accidents and sickness care may be processed.

(5) The archival retention period of documents related to processing and data transfer is set out in the University's Document Management Policy.

(6) Personal data may only be processed for clearly defined, legitimate purposes, for the exercise of rights and the fulfilment of obligations, to the extent and for the duration necessary for the fulfilment of the purposes. Only personal data that are necessary for the realization of the purpose of data processing and suitable for the achievement of the purpose may be processed. At all stages of processing, the purpose of the processing must be fulfilled, the collection and processing of data must be fair and lawful, and the processing must be performed in a transparent manner for the data subject.

(7) If the purpose of the processing ceases to exist or the processing is otherwise unlawful, the data must be erased. When data are erased, they are turned into an unrecognisable form, from which they cannot be restored.

(8) In the course of erasure, the facts relating to the cessation of processing shall be recorded. The detailed rules for the erasure of data are set out in the University's Document Management Policy.

(9) The University ensures adequate security of personal data by implementing appropriate technical or organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

(10) The accuracy and completeness, and - if deemed necessary in the light of the aim of processing - the up-to-dateness of the data must be provided for throughout the processing operation, and shall be kept in a way to permit identification of the data subject for no longer than is necessary for the purposes for which the data were recorded. The data owner defined is this Policy is responsible for this.

(11) The use for private purposes of personal data processed by the University or provided by another controller for the performance of the University's tasks is prohibited. Any staff member who infringes this provision shall be liable to disciplinary action.

(12) Any employee of the University who is a processing employee shall be liable to disciplinary action, damages, civil and criminal liability for the lawful processing of personal data of which they become aware in the course of their duties and responsibilities, and for the lawful exercise of their access rights to the University's records.

(13) Data processing employees are obliged to keep the personal data they have obtained. Only a person who has signed a confidentiality agreement may be employed in such a position.

(14) If a University employee becomes aware that personal data that they are processing is inaccurate, incomplete or out of date, they must rectify it or request its rectification from the employee responsible for the data.

Section 3 Legal ground and purpose of processing

(1) At the University, personal data may be processed, if

a) the data subject gave their express consent, in writing or by electronic means through the NEPTUN system, to the processing of their personal data in a recorded form, or

b) it is ordered by law, or

c) essential for the proper functioning of the University, the exercise of employer's rights, the organisation of programme and research, or

d) for the exercise of the rights and obligations of applicants, students, lecturers, researchers, teachers, employees, for the establishment, assessment and verification of entitlement to benefits, or

e) necessary for maintaining contact with former students of the University and for career monitoring, or

f) is necessary and proportionate for the protection of the vital interests of the data subject or of another person or for the prevention or elimination of an imminent threat to the life, limb or property of a person; or

g) the personal data have been expressly made public by the data subject and are necessary and proportionate for the purpose of the processing; or

h) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, ir

i) processing is necessary for the purposes of the legitimate interests pursued by University or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

(2) Unless the duration or periodic review of the necessity of the processing is specified by law or by a legally binding act of the European Union, the University shall review, at least every three years from the start of the processing, whether the processing of personal data processed by it or by a processor acting on its behalf or under its instructions is necessary for the purposes of the processing. The circumstances and the outcome of the review is documented by the University.

The documentation is kept for ten years after the erasure of the processed data and is made available to the National Authority for Data Protection and Freedom of Information upon request.

(3) Special data are processed by the University for the purpose of fulfilling the data subject's obligations and exercising their specific rights arising from the legal provisions governing employment and social security and social protection, as well as for occupational health purposes and to assess the employee's ability to work.

The University may also process special data where the data subject gives their explicit consent to the processing of their special personal data for one or more specific purposes, unless EU or Member State law provides that the prohibition on processing special data cannot be lifted by the data subject's consent.

(4) For processing special data, the University takes appropriate technical and organisational measures to ensure that, when performing the processing operations, only those persons who have the necessary access to the special data for the performance of their tasks in connection with the processing operation have access to the special data.

(5) The data subject has to be informed of the purpose of the processing and whether the provision of the data is voluntary or mandatory before the data are collected.

For *voluntary data provision*, the data subject has to be informed that participation in the provision of data is not compulsory.

For *mandatory data provision*, the legal provision or university policy imposing data processing must be indicated.

(6) Before or at the time of the start of the processing of personal data, the data subject must be informed, in a clear and intelligible manner, in sufficient detail and in an easily accessible format (web interface, NEPTUN), of all the facts relating to the processing of their data, in particular:

a) the name and contact details of the University and the University's representative and, where a processing operation is performed by a processor, the name and contact details of the processor,

b) contact details of the data protection officer,

c) purpose of the planned processing of personal data and legal ground of processing

d) where applicable, the fact that the University intends to transfer the personal data to a third country or an international organisation, the existence or absence of a European Commission adequacy decision and, in the case of data transfers under an adequacy decision, an indication of the appropriate and suitable safeguards and a reference to the means of obtaining a copy or the availability of a copy thereof.

e) the period for which the personal data are kept and, if this is not possible, the criteria for determining that period,

f) the recipients of the transfer of personal data processed or intended to be transferred,

g) the source of the collection of the personal data processed, where it is not collected directly from the data subject,

h) on the fact whether the data provision is voluntary or mandatory,

i) the rights of the data subject involved in processing and the means of enforcing those rights.

(7) [2]The information should also cover the rights and remedies of the data subject in relation to the processing.

(8) Employees of the University's departments who process personal data are required to keep the personal data they have obtained confidential as official and/or trade secrets. Only a person who has signed a confidentiality agreement may be employed in such a position.

(9) The University records personal data that are indispensable for

a) the proper functioning of the institution,

b) the exercise of the rights and obligations of applicants and students,

c) the organisation of the programme and research,

d) the exercise of employer's rights and the rights and obligations of lecturers, researchers and employees,

e) keeping the records required by law,

f) the establishment, assessment and verification of entitlement to benefits provided by law and the University's Rules for Organisation and Operation,

g) career monitoring of graduates.

(10) The University may process personal data in connection with employment, the establishment and fulfilment of benefits, discounts and obligations, for reasons of national security and for the purpose of managing the records specified in the national higher education act, to the extent appropriate for the purpose and for the purpose for which they are collected.

(11) In order to exercise the right to erasure, the personal data of the data subject must be **erased** without undue delay if.

a) the processing is unlawful, or

b) the data subject objects to the processing, except for mandatory processing, or

c) the purpose of the processing is no longer fulfilled or the further processing of the data is no longer necessary for the purpose of the processing, or

d) the period for which the data are stored expired, as defined by law, an international treaty or a legally binding act of the European Union, or

e) the legal basis for the processing ceased to exist and there is no other legal ground for the data processing,

f) it is ordered by law, a legal act of the European Union, a court or the National Authority for Data Protection and Freedom of Information.

(12) In the case provided for in paragraph 11(c), the obligation to erase does not apply to personal data whose data medium is subject to archival custody pursuant to the legislation on the protection of archival material.

(13) The scope of the data recorded, the purpose and duration of the data processing and the conditions for the transfer of the data recorded are governed by a separate set of procedures (Information Transfer Policy). The data recorded may be used for statistical purposes and may be transmitted to the official statistical service for statistical use.

Section 4 Recording of the processing activity

(1) All data processing at the University must be registered in a record (hereinafter data processing ledger) *(Annex 3)*. The first copy of the data processing ledger is kept by the head of the department responsible for data processing and the second copy by the data protection officer.

(2) The data processing ledger regulates and documents the most important facts and circumstances related to data processing for specific processing operations within the framework of the legislation and the University's regulations, in accordance with the principles of data protection as laid down in the Fundamental Law and the Regulation, in particular:

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

b) purpose of the processing,

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

d) if possible, the time limits foreseen for the erasure of the different categories of data,

e) if possible, a general description of the data security measures,

f) where applicable, information about the transfer of personal data to a third country or international organisation.

(3) In addition to paragraph (2)(a) to (f), where processing is performed using a processor, the name and contact details of the processor or processors and, where applicable, the name and contact details of the controller or the representative of the processor, as well as the categories of processing activities performed on behalf of each controller, must be recorded in the data processing ledger.

(4) The data protection officer and the competent controller review the accuracy of the data in the data processing ledger as necessary, but at least annually, and update it to reflect any changes that have occurred in the meantime. After the termination of the data processing, the data processing ledger must be archived and scrapped after 10 years of retention.

(5) Through the data protection officer, the University keeps records for the purposes of monitoring the measures taken in relation to the **personal data breach** and informing the Authority and the data subject, which include the following:

a) the nature of the personal data breach, including, where possible, the scope and approximate number of data subjects affected by the personal data breach,

b) the scope and approximate amount of personal data involved in the breach,

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

d) the likely consequences of the personal data breach and the measures taken to mitigate any adverse consequences,

and other data specified in the legislation requiring the processing.

Section 5 Privacy impact assessment, preliminary consultation

(1) Where a type of processing, in particular one using new technologies, is likely to present a high risk to the rights and freedoms of natural persons, taking into account its nature, scope, context and purposes, the controller conducts an impact assessment prior to the processing of personal data concerning the impact of the envisaged processing operations on the protection of personal data and on the fundamental rights of the data subjects.

(2) When performing the data protection impact assessment, the data controller must seek the professional advice of the data protection officer, or, if the data protection officer is prevented from doing so, the opinion of the Legal Office in legal matters, or the opinion of the IT Service Centre in IT security matters.

(3) The data protection impact assessment includes at least a general description of the envisaged processing operations, a description and the nature of the risks to the fundamental rights of data subjects identified by the controller, the measures envisaged to address those risks and the measures taken by the controller to ensure the exercise of the right to personal data.

(4) Where the data protection impact assessment concludes that the processing is likely to the controller consults the Authority prior to processing personal data, the controller consults the Authority prior to processing personal data.

Section 6 Rights of the data subject involved in processing and the enforcement thereof

(1) The data subject may request information from the University as to whether or not their personal data are being processed and, if such processing is ongoing, they have the right to request information about and access to the processing of their personal data and the processing of their personal data. Access must be ensured in such a way that the data subject is not made aware of the data of another person.

(2) Within the shortest possible period of time from the date of the request, but not exceeding 25 days, the controller shall decide on the data subject's request and notify the data subject of the decision in writing in an intelligible form and in writing or, if the data subject has submitted the request by electronic means, by electronic means (unless the data subject requests otherwise). The controller provides the data subject with information in writing in an intelligible form about the data processed by the controller or by a processor to whom the controller has delegated the processing, the purposes, legal ground and duration of the processing, the name and address of the processor, the activities of the processor in relation to the processing, who has received or is receiving the data and for what purposes, and, where the data have not been collected from the data subject, any available information about their source.

(4) Where there are reasonable doubts as to whether the person making the request is the same person as the data subject, the controller complies with the request after obtaining credible proof of the identity of the person making the request.

(5) The University may delay the exercise of the data subject's right of access, restrict the content of the information or refuse to provide it, in proportion to the aim pursued, in order to safeguard the interests specified by law. Where such a measure is taken, the controller shall inform the data subject in writing without delay.

(6) The data subject has the right to have inaccurate personal data relating to them **corrected** by the University without undue delay upon request. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The University is not obliged to rectify personal data if accurate, correct or complete personal data is not available to it and is not provided by the data subject, or if the accuracy of the personal data provided by the data subject cannot be established beyond reasonable doubt.

(7) The data subject has the right to have the University **restrict processing** at their request if one of the following conditions is met:

a) the data subject contests the accuracy of their personal data, in which case the restriction shall apply for the period of time necessary to allow the University to verify the accuracy of the personal data,

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

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

d) the data subject objected to the data processing; in such cases the restriction shall only apply to the time period necessary to determine whether the Controller's justified needs precede the needs of the data subject.

(8) Where processing has been restricted under paragraph (7), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(9) A data subject who has obtained restriction of processing pursuant to paragraph (7) shall be informed by the University before the restriction of processing is lifted.

(10) For processing based on non-mandatory data provision, the data subject may request the erasure of his or her processed data without giving reasons. The controller erases personal data concerning the data subject without undue delay, except in cases of mandatory processing.

(11) Where the controller refuses a request by the data subject to rectify, restrict or erase personal data concerning them, the data subject is informed in writing without delay of the fact of the refusal, the legal and factual grounds for the refusal, the rights of the data subject and the means of enforcing them.

(12) If the purpose of the management of personal data is direct marketing the data subject has the right to place objection at any time to the use of their personal data for this purpose, including profiling if it is made for the purpose of direct marketing. If the data subject places an objection to the use of their personal data for direct marketing purposes the personal data shall not longer be used for such purposes.

(13) In the event of a breach of their rights in relation to data processing, the data subject may turn to the head of the department performing the processing (director of the institute, heads of departments), or, if this is unsuccessful, to the Authority or to the courts, as provided for in the Infotv.

In the event of a dispute between the head of the department responsible for data processing and the data subject, the decision is made by the person exercising the employer's authority (the rector).

(14) The fact of providing the data must be recorded in the computerised or manual records in such a way that the date of the provision of the data, the legal title and the identity of the person requesting the data can be established (for 10 years after the processing). The legal consequences of any unlawful request for or use of data are borne by the person requesting the information.

(15) Where the University rectifies, erases or restricts the processing of personal data processed by it or by a processor acting on its behalf or at its instructions, it notifies the fact and the content of the action taken to that effect to all controllers and processors to whom it transferred the data prior to the action taken, in order to implement the rectification, erasure or restriction of processing of their own data.

(16) Where the University refuses a data subject's request for the rectification, erasure or restriction of the processing of personal data processed by the University or by a processor acting on its behalf or at its instructions, it informs the data subject in writing without delay

a) on the fact of the refusal, the legal and factual grounds for the refusal, and

b) on the rights to which the data subject is entitled under the Infotv. and the means of exercising them, in particular that the data subject may exercise his or her right to rectification, erasure or restriction of processing of personal data processed by the University or by a data processor acting on its behalf or on its instructions, with the assistance of the Authority.

Section 7 Intra-university data transfers, connection of processing

(1) Within the University's operational system, the personal data of employees and students, as well as of persons working under other employment relationships (in particular, lecturers employed under an assignment contract) may be transferred to the department performing the tasks to the extent and for the duration necessary for the performance of the administrative and organisational tasks related to the employment relationship, the performance of the assignment and the student status.

(2) In the course of project activities implemented by the University, personal data may be transferred to the department or person performing the task, to the extent and for the duration necessary for the performance of the tasks of the project, as specified in the privacy notice for the project concerned.

(3) Data processing for different purposes at the University may be temporarily linked only for legitimate purposes and in justified cases.

(4) The connection of processing operations must be registered in a record *(Annex 4)*, in which the following facts must be documented:

a) the name of the connected data processing operations,

b) the purpose and function of the connection,

c) the date and duration of the connection,

d) its legal ground (law, local regulations),

e) the name, position, department, office and telephone number of the person who performs the connection,

f) the scope and number of the data subjects by the connection,

g) the scope of the connected data,

h) the method of connecting (manual, computer, mixed),

i) data security measures.

(5) The first copy of the record shall be kept at the place of processing and the second copy shall be transferred to the University's data protection officer. The record must be kept for 10 years.

Section 8 Data transfer to the higher education information system

(1) The detailed rules for data transfer are set out in Section 18 and Annex 3, Annex 6 of the Nftv. and Sections 25-31 of Government Decree 87/2015 (9 April).

Section 9 Data transfer on request

(1) A request for a disclosure of personal data from an entity or individual outside the University may only be fulfilled if the data subject gave their written consent to this.

The data subject may also give such an authorisation in advance, which may be for a specified period of time and/or to a specified number of the requested bodies.

(2) The data transfer must be executed irrespective of the data subject's declaration, if required by law, in particular requests from authorities in civil and criminal matters - police, courts, prosecutors, customs and tax authorities, NAV, Pension Fund, and national security services. The competent data controller is obliged to inform the Rector of requests from these bodies, either directly or through their superior. The provision of data is subject to the approval of the Rector, with the exception of the provision of data on students. The rector may lodge a non-adjournable complaint with the competent minister against a request for data from the national security services.

(3) All data relating to a request from the national security services are state secrets pursuant to Section 42 of Act CXXV of 1995 on National Security Services, which may not be disclosed to any other body or person.

(4) The facts and circumstances relating to the provision of information pursuant to the request shall be documented by taking a record *(Annex 5)*. The record contains the following information:

a) name, postal address and telephone number of the body or person making the request,

b) the legal grounds for the data request or the data subject's declaration of consent:

d) the date of the data request,

e) the name of the data processing operation on which the data are based,

f) the name of the department providing the data,

g) data subjects:

h) scope of the requested data,

i) the method of the data transfer,

j) data security measures.

(5) The first copy of the record of the request must be kept at the place of processing and the second copy must be transferred to the University Data Protection Officer, or in case of their unavailability to the Legal Office. The record must be kept for ten years.

Section 10 Data transfers abroad

(1) Personal data may be transferred to a third country or international organisation when

a) the data subject gave their express consent to the international data transfer; or

b) the international data transfer is necessary for the purpose of the processing, and

c) the European Commission has established that the third country, a territory or one or more specific sectors of the third country, or the international organisation in question provides an adequate level of protection.

(2) Facts and circumstances relating to the data transfer abroad must be documented by a record *(Annex 6)*. The record contains the following information:

a) the recipient of the data transfer (name, postal address, telephone number),

b) the purpose of data transfer,

c) the legal grounds for the data transfer and the data subject's declaration:

d) the date of the data transfer,

e) the name of the department providing the data,

f) data subjects:

g) the scope of the transferred data,

h) the method of the data transfer.

(3) The first copy of the record of the data transfer abroad must be kept at the place of processing and the second copy must be transferred to the University's data protection officer. The record must be kept for ten years.

Section 11 Disclosure of personal data

(1) Disclosure of personal data processed at the University is prohibited, unless required by law or with the consent of the data subject.

(2) Statistical data about the University, including those based on personal data, may be disclosed without restriction.

Section 12 Data security policies and measures

(1) In order to ensure an adequate level of security for the personal data processed and to safeguard the fundamental rights of data subjects, the University or the data processor in the course of its activities must ensure the security of the data and must take technical and organisational measures appropriate to the level of risk and establish the necessary rules of procedure, which are necessary to enforce the Infotv., the Regulation, this Policy and other data protection and confidentiality rules, in order to ensure a level of data security appropriate to the level of risk.

(2) The data must be protected by appropriate measures, in particular against unauthorised access, alteration, disclosure, erasure, destruction, destruction or damage.

(3) The purpose of data security policies and measures is to protect data and data media against damage, deterioration, destruction and unauthorised access.

(4) Data security policies are set out in the University's IT and Information Security Policy.

Section 13 Audit

(1) Compliance with data protection rules is continuously monitored by the heads of the departments responsible for data management and processing, in particular with the provisions of this Policy.

(2) The head of the department takes immediate action to put an end to any violation of the law or of the provisions of the Policy. Particularly serious or repeated misconduct may lead to disciplinary proceedings.

(3) The University's internal auditor may inspect and request information on all documents relating to internal audit investigation topics ordered by the rector.

Section 14 Data protection officer

(1) The rector appoints a **data protection officer** with professional competence and, in particular, with an adequate level of knowledge of data processing law and practice, to enforce the legislation and regulations on records and data management. The data protection officer may be an employee of the University or may perform his or her duties under a service contract.

(2) Tasks of the data protection officer:

a) to inform and advise the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions,

b) monitors compliance with the legal requirements, legislation and this Policy in relation to the processing of personal data and, where necessary, makes proposals to ensure compliance with the legal environment,

c) plays a role in increasing the data protection knowledge and awareness of university employees involved in data processing operations,

d) on request, provides technical advice on the data protection impact assessment and monitors the conduct of the impact assessment,

e) facilitates the exercise of data subjects' rights, in particular by investigating complaints by data subjects about the processing of their personal data, and, if necessary, by taking the necessary measures at the controller to remedy the complaint,

f) liaises and cooperates with the Authority,

g) contributes to the creation and updating of internal data protection and data security policies.

(3) The data protection officer assists and directs the work of the departments responsible for data processing and controls the lawfulness of data processing at the University by providing advice and opinions. They perform audits of specific processing operations as necessary, but at least once a year. The data protection officer informs the rector in writing of the findings of the audit.

(4) The University supports the data protection officer in the performance of their duties by providing them with the necessary resources, which are necessary for the performance of those tasks, for access to personal data and processing operations and for maintaining the data protection officer's level of expertise. The data protection officer has the right of access to the processing of data and to the records and data processing ledgers of processing in all departments of the University. They may request documented oral or written information from the head of any department or staff member of the University. Personal data obtained during the audit are covered by the obligation of professional secrecy.

(5) If a breach of the law or of this Policy is detected, the data protection officer requests the controller to put an end to it, if necessary, helps to restore the lawful situation.

(6) If the data protection officer is unavailable, the duties of the data protection officer are temporarily performed by the Legal Office for the duration of the unavailability, and IT matters are handled by the ISZK (IT service provider).

Section 15 Rules on access to data of public interest and public data processed by the University

(1) Anyone may make a request for access to data of public interest not included in the publication lists and data which are in the public interest, orally, in writing or electronically.

Requests should be made to the University at the following contact details:

In writing to the University of Dunaújváros, Rector's Cabinet, 2400 Dunaújváros, Táncsics M. u. 1/A

Electronically: hivatal@uniduna.hu

Orally and in writing: at the University Rector's Office, during working hours.

A record must also be kept of the oral request.

(2) Where the data request is unclear, the controller invites the requester to clarify the request.

(3) The data request must be made in a way that is comprehensible and indicated by the data requester.

(4) Written data requests must be transferred to the rector and the data protection officer as soon as possible after receipt and to the head of the department for an opinion (data request). The head of the requested department is obliged to provide the rector with the answer (the requested data) within 3 working days and at the same time prepare the answer to be given to the requester. If the request is for the provision of data in the public interest and there is a concern about the feasibility of the request, the opinion of the internal data protection officer must be sought without delay.

(5) Requests for data in the public interest must be complied with as soon as possible and within a maximum of 15 days.

a) In the event of a large volume or number of requests, the time limit may be extended once by a maximum of 15 days, and the data requester must be informed of this within 15 days of receipt of the request.

b) The University is not obliged to comply with the data request to the extent that it is identical to a data request for the same set of data submitted by the same requester within one year, provided that there has been no change in the data in the same set of data.

c) The University is not obliged to comply with a data request if the requester does not provide their name, or in the case of a non-natural person, their designation, and the contact details at which any information and notification relating to the data request may be provided.

(6) Within 15 days of receipt of the request, the University informs the requester in writing or, if the request was received electronically or if the electronic mail address is indicated in the request, by electronic mail, of the refusal to fulfil the request and the reasons for the refusal.

(7) The University keeps a record of rejected requests and the reasons for rejection, and informs the Authority of the information contained therein by 31 January each year.

(8) The requester may obtain a copy of the document or part of a document containing the requested data, regardless of the way in which it is stored. The cost of making a copy may be reimbursed up to the amount of the costs incurred, the amount of which is notified to the requester by the University prior to the provision of the copy. The requester declares whether they maintain their request within 30 days of receiving the information. The period from the time the information is provided to the time the University receives the requester's statement does not count towards the time limit for fulfilling the request.

If the requester maintains their request, they must pay the reimbursement to the University within a time limit set by the University, which must be at least 15 days.

(9) The University notifies the requester that the document or part of a document requested as a copy is of significant volume, the amount of the fee and the options for fulfilling the data request without making copies within 8 days of receipt of the request.

(10) The University executes the request for a copy of a document or part of a document of significant length within 15 days of the date of payment of the fee.

(11) If the document containing data of public interest also contains data which are not known to the requester, the copy of the document must be made unrecognisable.

(12) The data request must be made in a form and manner that is comprehensible and, where the University is able to do so without disproportionate difficulty, in the form and manner requested by the requester. If the information requested has already been disclosed in electronic form, the request may be met by indicating the public source of the information. A data request may not be refused on the grounds that it cannot be met in an intelligible form.

(13) A request for access to data of public interest may not be refused on the grounds that the requester, whose mother tongue is not Hungarian, formulates the request in their mother tongue or in another language which they understand.

(14) The requester may apply to the courts for a review of the amount of the fee for the execution of the request for access to data of public interest, in the event of the refusal of the request for access or of the unsuccessful expiry of the time limit for execution or of the extension of the time limit by the University pursuant to paragraph (5), and for the amount of the fee for the execution of the request.

(15) The legal action must be brought against the University before the competent court within 30 days of the date of notification of the rejection of the request, the expiry of the time limit without result or the expiry of the time limit for the payment of the reimbursement of costs. The procedure is an extraordinary one.

(16) The Rector's Office is responsible for coordinating and responding to requests for data of public interest, while the content of the data is compiled by the Legal Office.

Section 16 Rules on the disclosure of information subject to mandatory disclosure

(1) The University is obliged to promote and ensure the provision of accurate and prompt information to the public on matters within its competence, in particular on the state budget and its implementation, the management of state property, the use of public funds and the contracts concluded for this purpose, the granting of special or exclusive rights to market operators, private organisations and individuals.

(2) According to the Infotv., the University is obliged to disclose data of public interest on its official website (www.uniduna.hu) in digital form (date, scope), accessible to anyone, without identification, without restriction, in a printable and in a way that can be copied in detail without loss or distortion of data, free of charge for viewing, downloading, printing, copying and network data transmission (hereinafter electronic disclosure). Access to the disclosed data may not be linked to the disclosure of personal data.

(3) Unless otherwise provided by the Infotv. or other legislation, data published electronically may not be removed from the website. In the event of the dissolution of the University, the obligation of disclosure falls on the successor of the University.

(4) The University shall disclose the information set out in the general publication list in *Annex 7* as specified in the Annex, in the relevant structure related to its activities.

(5) Legislation may specify other information to be disclosed for certain sectors, for the type of body having public service functions (hereinafter: special disclosure list).

(6) After consulting the Authority, the Rector may specify additional mandatory data to be disclosed, and legislation with effect for a body having public service functions, bodies subject to their management or supervision, or parts thereof (hereinafter specific disclosure list).

(7) The rector reviews the disclosure list issued by them pursuant to paragraph (6) at least annually on the basis of the data of the data requests concerning data of public interest not included in the disclosure list, and supplements it on the basis of data requests arising in a significant proportion or volume.

(8) The disclosure list may also specify the frequency of disclosure, depending on the nature of the information to be disclosed.

(9) The Authority may also propose the establishment of, or additions to, special and specific disclosure lists.

(10) The University is responsible for the transfer of the descriptive data of the websites, databases and records containing data of public interest under its management to the Minister responsible for ensuring the infrastructural feasibility of public administration IT and for the regular updating of the data of public interest transferred, and is also responsible for the content of the data of public interest transferred to the unified public data retrieval system and for the regular updating of the data of public interest transferred.

(11) The maintenance of a list of databases or records containing data of public interest and the connection to the unified public data retrieval system do not exempt the data source from the obligation of electronic disclosure.

(12) The tasks of disclosure, rectification, update and removal are performed by the data protection officer, the website administrator, in conjunction with the relevant managers.

(13) The Data Protection Officer reports in writing to the rector once a year on the fulfilment of the obligations related to the implementation of the Infotv.

II. SPECIAL PART

Specific processing operations

Section 17 Personal and special data recorded and processed by the provider of the higher education institution

(1) Pursuant to Annex 3, point IV of the Nftv., personal and special data transferred or made directly accessible to the provider of the higher education institution by the higher education institution, either individually or through its IT system, for the purpose of performing tasks related to the management of the provider of the higher education institution and exercising the rights of the provider of the higher education institution.

(2) Duration of processing: five years from the date of data transfer.

3. The data listed in paragraph (1) may be transferred to: the court, the police, the public prosecutor's office, the bailiff, the public administration (data necessary for the decision of a specific case); the persons entitled to monitor the provisions on employment (employment related data);

the National Security Service (all data necessary for the performance of the tasks specified in the Nbtv.); the Student Loan Centre (data related to the lawful disbursement of student loans and the continuation of studies); data which are in the public interest pursuant to Section 26 (3) of the Data Protection Act2 for the purpose of fulfilling a request for access to data addressed to the provider pursuant to Section 28 of the Avtv2.

Section 18 Records of student data

(1) Student records are data processing for the documentation of facts concerning the student status, the legal basis of which is the Nftv., the University's Rules for Organisation and Operation and the student regulations, in particular the Study and Examination Regulations.

(2) The student records contain the details of all students enrolled in the University's basic, additional and postgraduate specialisation programmes. All data relating to the student status, studies and related finances may be recorded in the records for each student.

(3) The personal and special data of the student records specified in Section 18 may be used for the performance of organisational and administrative tasks related to the fulfilment of the student's study and examination obligations, as well as the determination, payment and payment of study grants and tuition fees, and may be used for statistical purposes as specified by law and may be transferred to the official statistical service for statistical purposes.

Purpose of processing: pursuant to Section 18 (1) of the Nftv. The University may process personal and special data only in connection with the legal relationship, the establishment and fulfilment of allowances, benefits and obligations, for reasons of national security, to the extent necessary for the purpose and for the purpose for which they are collected.

Duration of processing: eighty years from the date of the notification of the termination of the student status.

(4) In order to determine the various benefits (study grant, social support, aid, etc.) for the student, the name of the parent (family keeper), address of the permanent and temporary residence, telephone number, as well as data proving the income and social status of the parent (breadwinner) and the student are required, the controller of which is the University Student Self-Government.

(5) The admissions database and the data provided by the student at the registration for the semester provide the basic data for the student record. The data generated during the admission procedure must be deleted by the end of the academic year at the latest, after being transferred to the student record, with the exception of the list of final admission results.

(6) The University may process personal and special data as defined in Section 19 of these Regulations, recorded and processed on the basis of student grant contracts, for the purpose of monitoring and controlling the fulfilment of the obligations undertaken by the student on a state (partial) study grant, to the extent and for the purpose for which they are intended. The data may be processed for five years from the date of termination of the study grant contract.

Section 19 Personal data of students

(1) The personal and special data of students processed by the University (as defined in Annex 3 of the Nftv.) are the following:

a) the student's name, name at birth, mother's name, place and date of birth, citizenship, register domicile, address, mailing address and telephone number, in case of a non-Hungarian citizen, the legal title of the student's stay in Hungary and the certificate of residence, based on separate law in case of a student having the right to free movement and residence, the title and number of the document certifying the right of residency;

b) data relating to student status, in particular

- data relating to the admission (data referred to in Annex 3, point 1/B of the Nftv.),
- assessment and qualification of the student's studies, examination data,
- data on the student's disciplinary and compensation cases,
- data on the student competency assessment and its results,

d) in order to determine the various benefits (study grant, social support, tax certificate. aid, etc.) for the student, the name of the parent (breadwinner), address of the permanent and temporary residence, telephone number, as well as data proving the income and social status of the parent (breadwinner) and the student,

e) data related to student career monitoring (DPR - graduate career monitoring system)

f) other data with the consent of the data subject.

(2) The data listed may be used for statistical purposes and may be transferred in a non-personally identifiable form for statistical purposes. Data from the records of students' names, date and place of birth, place of residence and place of stay must be transferred to the National Higher Education Information Centre in accordance with the provisions of the Privacy Act.

Section 20 Personal and special data recorded and processed under student study grant contracts

(1) Data registered by the National Higher Education Act, the student with a state (partial) study grant

a) natural person identification data, tax identification number, social security number,

b) address details (residence and domicile),

c) details of the establishment and duration of domestic employment relationship(s),

d) data on the record as a jobseeker as defined in the Act on the Promotion of Employment and Unemployment Benefits and on the duration of time spent as a jobseeker,

e) details of the duration of the payment of the maternity benefit,

f) details of the duration of the payment of the child care allowance,

g) details of the duration of the payment of the child care benefit,

h) the reason and date of removal from the register of identity and address,

i) details of the reduced capacity for work and its duration,

j) citizenship,

k) e-mail address,

l) information on the higher education programme and student status.

(2) The body responsible for recording the fulfilment of the conditions of the Hungarian state (partial) study grant is entitled to process the data. The data may be processed for five years from the date of fulfilment of the conditions set for the student. If the student status has not been established, the applicant's data may be kept for one year from the date of application in accordance with the first subparagraph of Section 18 (1) b).

Section 21 Processing student data

(1) The Student Administration Office (hereinafter Hungarian abbreviation TH) is the controller of student data.

(2) The TH authorises the departments responsible for education to process personal data relating to studies, who exercise control over the data relating to the commencement of studies, progress, examination results, etc. through the administrators of the department and the lecturers.

(3) Within the University, the student records may be used to provide information to the University Student Self-Government and the Chairman of the Student Welfare Committee, as well as to the department responsible for determining the student's study and examination obligations, the social and other benefits and services available to the student, and the payment obligations to be fulfilled by the student.

(4) Further rules on student records are laid down in the student data processing ledger.

(5) The University may process personal and special data only in connection with the legal relationship, the establishment and fulfilment of allowances, benefits and obligations, for reasons of national security, for the purpose of managing the records specified in the Nftv, to the extent necessary for the purpose and for the purpose for which they are collected.

(6) Duration of processing: for eighty years from the date of the notification of the termination of the student status.

(7) The Vocational Training Institution maintained by the University has its own data processing regulation.

Section 22 Record of personnel data

(1) Personnel records are data processing for the documentation of facts relating to the employment relationship, the legal basis of which is the Act on National Higher Education (Nftv.), Act I of 2012 on the Labour Code, the University's Rules for Organisation and Operation and the Collective Agreement.

(2) The personnel records contain the data of all full-time and part-time lecturers, academic staff, researchers and other employees of the University who are in employment relationships. The data that can be entered in the records on the data subjects are as follows, in accordance with the Annex to the Higher Education Act and the Labour Code:

a) name, place and date of birth, and citizenship;

b) permanent and temporary address, telephone number;

c) employment data, especially:

- graduation, vocational qualification, conditions of employment, exemption from qualification requirements,
- further training, specialised further training, vocational qualifications obtained in further training,

- scientific degrees and titles,
- foreign language skills,
- deed of appointment, position, job description,
- managerial assignments,
- period of traineeship, examination, probationary period,
- disciplinary proceedings, penalty, exemption,
- wage grade,
- scientific research (publication), artistic and creative activity, scientific relations,
- time worked, time spent as a civil servant, time counted towards employment relationship, classification related data,
- honours, awards and other recognitions received by the employee,
- job, assignment to a task outside the scope of the job, additional employment relationship, disciplinary sanction, compensation,
- time worked, overtime, basic salary, allowances (by title), salary supplement, commission, and the amount owed and the person entitled thereto,
- holidays, allocated holidays,
- payments made to the employee and the related tittles,
- benefits provided to the employee and the related titles,
- debts of the employee towards the employer and the related titles.

(3) Data from the personnel records can be used to establish facts about the employment relationship, to verify classification requirements and to provide statistical data. Data from the records may only be provided for statistical purposes in a way that does not allow for identification of the individual.

(4) The data subject provides the personal data in the personnel records. The primary survey occurs at the time the employment relationship is established, at the same time as the privacy notice and consent declarations are requested.

(5) Personal data relating to religious or philosophical affiliation or proof of such affiliation as a condition of application cannot be recorded. Other data can be recorded with the consent of the data subject.

(6) Of the data contained in the personnel records, the name of the employer, the name of the employee and the data concerning their classification are in the public interest and may be disclosed without the employee's prior knowledge and consent.

(7) In addition to the data subject, the following persons are entitled to consult the personal records kept by the employer or to receive data from them for the purpose of performing their duties as defined by the law applicable to them:

a) the person exercising employer's rights over the employee,

b) the rating manager,

c) the body which exercises control or supervision of legality within the scope of its functions,

d) the court in connection with labour, civil or administrative proceedings,

e) the investigating authority, the prosecutor and the court in criminal proceedings against the employee,

f) a member of the staff of the body responsible for personnel, labour and payroll matters within the scope of their duties,

g) the tax authority, the pension insurance administration and the health insurance body, the body that investigates industrial accidents and the labour inspectorate.

(8) The University may process personal and special data only in connection with the employment, the establishment and fulfilment of allowances, benefits and obligations, for reasons of national security, for the purpose of managing the records specified in the Nftv, to the extent necessary for the purpose and for the purpose for which they are collected.

(9) Duration of processing: five years from the end of employment.

Section 22/A Employee competence data

(1) In order to ensure the more efficient performance of its human resources strategy, the University processes data on the CV, ORCID or other researcher ID, data on the participation in projects, and data provided by the data subject by completing a questionnaire, in addition to the data of employees listed in Section 22, as specified in the privacy notice.

Section 23 Record of HR Services data

(1) HR Services records are data processing for the documentation of facts relating to the employment relationship, the legal basis of which is the Nftv., Act I of 2012 on the Labour Code, the University's Rules for Organisation and Operation and the Collective Agreement.

(2) The data in the HR Services records can be used to establish the facts about the employee's employment relationship, to verify classification requirements, for payroll, social security administration and statistical data provision.

(3) The HR Services records contain data on all employees of the University. The data that can be entered in the records on the data subjects according to the Annex to the Nftv:

a) name, place and date of birth, and citizenship,

b) permanent and temporary address, telephone number;

c) employment data, especially:

- graduation, vocational qualification, conditions of employment, exemption from qualification requirements,
- further training, specialised further training, vocational qualifications obtained in further training,
- scientific degrees and titles,
- foreign language skills,
- deed of appointment, position, job description,

- managerial assignments,
- period of traineeship, examination, probationary period,
- disciplinary proceedings, penalty, exemption,
- wage grade,
- scientific research (publication), artistic and creative activity, scientific relations,
- time worked, time counted as employment relationship on the basis of civil servant status, classification related data,
- honours, awards and other recognitions received by the employee,
- job, assignment to a task outside the scope of the job, additional employment relationship, disciplinary sanction, compensation,
- time worked, overtime, basic salary, allowances (by title), salary supplement, commission, and the amount owed and the person entitled thereto,
- holidays, allocated holidays,
- payments made to the employee and the related tittles,
- benefits provided to the employee and the related titles,
- debts of the employee towards the employer and the related titles.

d) data that may be processed within the scope, to the extent and for the duration regulated by the Act on Benefits for Persons with Disability.

e) other data with the consent of the data subject.

(4) The personal data of the employee, issued by the criminal records body to prove the employee's criminal record and that they are not subject to a disqualification from employment, will be processed until the date of the decision to establish the employment relationship or □□ , in the case of an employment relationship, □ until the termination of the employment relationship.

(5) The data subject provides the data of the HR Services records. The primary survey occurs at the time the employment relationship is established, at the same time as the privacy notice and consent declarations are requested.

Section 24 Processing of personnel and HR Services data

(1) The controller of the personnel data and HR Services data is the Labour Office.

(2) The registered is managed in a mixed structure, both on computer and with a manual method. The controllers are responsible for data security. The data protection officer of the University and the administrator appointed by the Head of the IT Services Centre assist in ensuring the security of the data stored on the computer.

(3) Within the University, data from the records of personal data can only be provided to the rector and the heads of the departments and data controllers/processors responsible for personnel matters where the lecturer is actually engaged in teaching or scientific research.

(4) Some of the data in the personnel records are also stored in a computerised institutional directory. The data subject must be informed of the scope of the data stored in the directory.

(5) The institutional directory can be integrated into directory systems that work on the federation principle to facilitate mobility of lecturers, researchers and students.

The directory integration techniques that work on the federation principle do not imply data exchange between the federated organisations. The data subjects must be notified of the establishment of the federation.

(6) Further rules on the personal records are laid down in the personal data processing ledger.

Section 25 Processing with camera system

(1) **Data** of the Controller

Controller: Technical Service Centre

Person responsible for processing: director of operations and services

(2) Legal grounds and purposes of processing: the 0-24 hour camera surveillance is used primarily for the purpose of asset protection, in compliance with the principles of the Infotv. and the relevant provisions of Act CXXXIII of 2005.

(3) The controller processes the facial image and voice of the data subject during the surveillance by camera. The cameras installed are capable of capturing and recording images of a quality that allows for the unique identification of persons within the University building and its premises.

(4) **Duration of processing**: the recorded data are erased within three working days after the recording, unless otherwise provided by law.

(5) The **areas monitored** by the camera:

a) Indoor cameras were installed in the common areas of the educational buildings (corridors, passageways, lobbies, other common areas).

b) Outdoor cameras monitor entrances

c) A camera system was also installed on floors I-III of the DGY35 building of the university dormitory.

(6) **Data security measures**: the recording is recorded and stored on a password-protected and virus-protected closed system on a computer. The data can be accessed by the authorised staff of the University's Technical Service Centre and, in the event of technical failures or maintenance, by the security company contracted by the University (Multi Alarm Zrt.; office: 2400 Dunaújváros, Dózsa György út 48., ground floor 1.)

Section 26 University of Dunaújváros Alumni processing

(1) The main goal of the University Alumni System is to build and strengthen the relationship between the University and its predecessors, former students, lecturers, researchers and the University, and to cultivate the traditions of Selmecbánya.

(2) Joining the Alumni System is voluntary and is accomplished by registering on the alumni.duf.hu portal.

(3) The further purpose of the processing and the scope of the data processed are defined in a separate policy.

Section 27 Processing related to accommodation service by University of Dunaújváros

(1) Pursuant to Section 9/H of Act CLVI of 2016 on the State's Responsibilities Regarding the Development of Tourism Regions, from 1 September 2021, our guests using the University's accommodation services must bring their identification document with them, regardless of age, and allow the receptionist to scan it with our document scanner at check-in to record their details.

(2) Failure to present this document will result in the accommodation provider refusing to provide the accommodation service on grounds of the above legislation.

III. PART

CLOSING PROVISIONS

Section 28 Entry into force

(1) The Senate approved this policy by its resolution 54-2021/2022 (17.05.2022), and simultaneously all former regulations existing on this topic are repealed.

(2) This Policy takes effect on 18.05.2022.

(3) The University discloses this Policy on its website, in a manner usual locally.

(4) The access route of this Policy is the following:

N:\3 - Szabályzatok\ ÉRVÉNYES SZABÁLYZATOK

Dunaújváros, 17.05.2022

Dr. habil István András
Rector
Chairman of the Senate
[Stamp: University of Dunaújváros
1. Dunaújváros]

Annex 1:

Procedure for the processing of personal data

(1) Personal data may only be processed by persons authorised to do so by virtue of their job title or managerial mandate. Personal data may only be processed by persons authorised to do so by virtue of their job title or managerial mandate. Documents containing personal data may only be consulted for a specific purpose by those authorised to do so by virtue of their position or managerial mandate.

(2) Employees who process personal data and who are authorised to consult documents containing personal data are obliged to keep the personal data they have access to as confidential. Only a person who has signed a confidentiality agreement may be employed in such a position.

(3) Personal data must be stored in a lockable cabinet or, in absence thereof, in a lockable room, and an access form must be created for each authorised person to consult these documents, which form is annexed to this Policy. The right of access to files containing personal data must be certified.

(4) Documents containing personal data may be transferred electronically only through the University's mail system; no other mail system may be used for the transmission of official matters. These data may be stored electronically in such a way that access to them is restricted to those authorised by their job title or by virtue of their managerial mandate.

Annex 2

Scope and level of access to personal data by persons authorised to process and access such data by virtue of their position or managerial mandate

(1) All rights to process and access personal data relating to employment:

Rector

Internal Audit Manager

Director General for Finance

Labour Office Manager and staff

Finance Office Manager and staff

Accounting Office Manager and staff

Controlling

Head of the Rector's Office

Legal Office Manager, in legal matters involving individuals

(2) The right to process and access all personal data related to the employment in the project, in addition to the above, during the project activity and its preparation:

- managers (manager, technical manager, financial manager), assistant project managers for the project.

(3) In matters falling within its competence: members of the Provider, the Senate, the Management Conference, the Matrix Conference

(4) In matters concerning students: heads and staff of units under the Vice-Rector for Education.

(5) The right to process and access all personal data is reserved to the managers listed in the Rules for Organisation and Operation (Hungarian abbreviation SZMR) in respect of the persons under their control.

(6) In respect of matters within their competence: and in respect of personal data relating thereto, the chairpersons and members of committees attached to the University Senate.

(7) For personnel selection assessments: the chairperson and members of the assessment/evaluation committee with regard to the personal data of the candidate necessary for the assessment.

(8) Foundation for the University of Dunaújváros: the members of the Board of Trustees and the members of the Supervisory Board of the Foundation with regard to applications, study grants and prizes;

Annex 3

DATA PROCESSING LEDGER
(*To be completed in duplicate*!)

1.	Controller: University of Dunaújvárosi, 2400 Dunaújváros Táncsics M. u. 1/a Represented by: .....rector Data protection officer's name, contact details: .....adatvedelem@uniduna.hu			
2.	Department (where the data are processed):			
3.	Purpose of the processing:			
4.	Legal ground of the processing:			
5.	Category of data subjects (public employee, student, other):			
6.	Scope and list of data recorded:			
7.	Names and titles of persons authorised to have access:			
9.	Source of the data (directly from the data subject or from another source):			
10.	Method of data processing (to be underlined)	Manual processing Automated processing Processing in mixed system	Detailed description:	
11.	Place of processing *(to be completed if different from the department responsible for processing)*:			
12.	Processing operations (to be underlined):		Data collection and recording Data storage Amendment Update Organisation Selection Transfer Disclosure Erasure Other operation:	
13.	When data supply is regular *(For which body? For which data? How regularly?)*	Name of the body:	Data provided:	Regularity:
14.	Data security rules and measures:			
15.	Do data transfers of personal data to third countries or international organisations occur? (If yes, the description thereof):			
16.	Data erasure (scrapping) date:	Data cannot be erased	Erasure date:	
17.	Check processing:	Check date:	Checked by:	
18.	If a data processor is used, the name(s) and contact details of the data processor(s): Name and contact details of the data processor's representative:			
Check date:	Checked by:			
Dated:				

…… ……

data protection officer manager responsible for processing

Annex 4

RECORD **ON THE CONNECTION OF PROCESSING ACTIONS** (*To be completed in duplicate*!)				
1.	Name of the connected data processing:			
2.	The name, position, department, office and telephone number of the person who performs the connection:			
3.	The purpose and function of the connection:			
4.	The legal grounds for the connection and the data subject's consent:			
5.	The date of the connection:			
6.	The scope of the connected data:			
7.				
8.				
9.	Scope and number of data subjects:		persons	
10.	The method of connection (to be underlined):	Traditional transfer Network transfer Transfer in mixed system	Detailed description:	
11.	Data security rules and measures:			
12.	When data supply is regular *(For which body?* *For which data?* *How regularly?)*	Name of the body:	Data provided:	Regularity:
Dated:				

…… ……

data protection officer manager responsible for processing

1. copy – the manager of the department responsible for data handling/processing
2. copy – data protection officer

Annex 5

RECORD ON DATA PROVISION ON REQUEST (*To be completed in duplicate*!)				
1.	Name, postal address and telephone number of the body or person making the request,			
2.	The purpose of the data request:			
3.	The date of the data request:			
4.	Legal ground for data transfer *(underline as appropriate)*: a) The data subject gave their express consent to the data transfer. b) The data transfer is necessary for the purpose of the processing.			
5.	Processing on the basis of which the data is provided, source of the data:			
6.	Name of the department performing the data provision:			
7.	Scope and number of data subjects:		persons	
8.	Scope of requested data:			
9.	The method of the data transfer:	Traditional transfer Network transfer Transfer in mixed system	Detailed description:	
10.	Data security rules and measures:			
11.	If connecting is frequent: *(For which body?* *For which data?* *How regularly?)*	Name of the body:	Data provided:	Regularity:

Dated:

…… ……

data protection officer manager responsible for processing

……

data requester (if it is submission in person)

1. copy – the manager of the department responsible for data handling/processing
2. copy – data protection officer

Annex 6

<table>
<tr><td colspan="4">RECORD OF DATA REPORTING ABROAD
(To be completed in duplicate!)</td></tr>
<tr><td>1.</td><td colspan="3">The recipient of the data transfer (name, postal address, telephone number):</td></tr>
<tr><td>2.</td><td colspan="3">The purpose of data transfer:</td></tr>
<tr><td>3.</td><td colspan="3">The date of the data transfer:</td></tr>
<tr><td>4.</td><td colspan="3">The legal ground of the data transfer*:
a) The data subject gave their express consent to the international data transfer.
b) The international data transfer is necessary for the purpose of the processing.</td></tr>
<tr><td>5.</td><td colspan="3">Name of the department performing the data provision:</td></tr>
<tr><td>6.</td><td colspan="3">The scope and number of data subjects concerned by the data transfer: persons</td></tr>
<tr><td>7.</td><td colspan="3">The scope of the transferred data:</td></tr>
<tr><td>8.</td><td>The method of the data transfer:</td><td>Traditional transfer
Network transfer
Transfer in mixed system</td><td>Detailed description:</td></tr>
<tr><td>9.</td><td colspan="3">Data security rules and measures:</td></tr>
<tr><td colspan="4">Dated:</td></tr>
</table>

…… ……

data protection officer manager responsible for processing

* Personal data may be transferred to a third country or international organisation when
  a) the data subject gave their express consent to the international data transfer; or
  b) the international data transfer is necessary for the purpose of the processing, and
  c) the European Commission has established that the third country, a territory or one or more specific sectors of the third country, or the international organisation in question provides an adequate level of protection.

1. copy – the manager of the department responsible for data handling/processing
2. copy – data protection officer

Annex 7

GENERAL DISCLOSURE LIST

I. Organisational, personnel data

Data		Update	Storage	Responsible
1.	The official name, registered office, postal address, telephone and fax numbers, e-mail address, website and contact details of the body having public service functions	Immediately after the changes	Previous state to be erased	Head of the Rector's Office
2.	Organisational structure of the body having public service functions with its departments, the tasks of the individual departments	Immediately after the changes	Previous state to be erased	Head of the Rector's Office
3.	Names, titles and contact details (telephone, fax and e-mail) of the heads of the body having public service functions and the heads of the departments	Immediately after the changes	Previous state to be erased	Head of the Rector's Office
4.	The name, contact details (telephone, fax, e-mail) and opening hours of the contact person in charge of the organisation	Immediately after the changes	Previous state to be erased	Head of the Rector's Office
5.	For corporate bodies, the number, composition, names, titles and contact details of the members of the body	Immediately after the changes	Previous state to be erased	Head of the Rector's Office
6.	Name and details of other body having public service functions responsible for or subordinate to the public task under the direction, control or supervision of the body having public service functions, as specified in point 1	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
7.	The name, registered office, contact details (postal address, telephone and fax numbers, e-mail address), field of activity, name of the representative of the entity which is majority-owned or participates in the body having public service functions, and the extent of participation of the body having public service functions	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
8.	Names, registered offices, contact details (postal address, telephone and fax numbers, e-mail address), founding documents, members of the governing body of public foundations established by a body having public service functions	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
9.	Name of the budgetary body set up by the body having public service functions, its registered office, the legislative act or decision establishing it, the statutes of the budgetary body, its director, the contact details of its website, its operating licence	Immediately after the changes	Keeping the previous state in the archive for 1 year	Not applicable for the University

10.	The names of the newspapers established by the body having public service functions, the name and address of the editorial board and publisher, and the name of the editor-in-chief	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
11.	The data of the superior or supervisory body of the body having public service functions, the body competent to hear appeals against decisions of the public authority or, failing this, the body exercising control over the legality of the body having public service functions, as specified in point 1.	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office

II. Data on activity, operations

Data		Update	Storage	Responsible:
1.	The full text in force of the basic legislation, public law and regulations governing the body having public service functions, the organisational and operational rules or order of business, the data protection and data security policy, which define the tasks, powers and core activities of the body.	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
2.	The designation and content of the public services provided by the body having public service functions or financed from its budget, the arrangements for accessing them, the level of charges for public services and the benefits accruing from them.	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
3.	Descriptive data of the databases or records maintained by the body having public service functions (name, format, purpose, legal ground, duration of data processing, data subjects, source of data, questionnaire to be filled in case of questionnaire survey), identification data of the records to be registered in the data protection register pursuant to the Infotv.; types of data collected and processed by the body having public service functions in the course of its core business, means of access, costs of copying.	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
4.	The title, subject of the public publications of the body having public service functions, how they are accessed, whether they are free of charge and the amount of any reimbursement.	Quarterly	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
5.	The procedure for the preparation of decisions of the corporate body, the method of public participation (opinion), the rules of procedure, the place and date of the meetings of the corporate body	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office

	furthermore the publicity of its decisions, records of its meetings and summaries thereof; details of the voting of the body, unless restricted by law.			
6.	Notices and announcements published by the body having public service functions.	Continuously	By keeping it in the archive for at least 1year	Head of the Rector's Office
7.	Technical descriptions of tenders published by the body having public service functions, the results thereof and the reasons for them.	Continuously	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
8.	Public findings of investigations and audits relating to the core business of the body having public service functions.	Immediately after receiving the report of the investigation.	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
9.	The procedures for dealing with requests for access to data of public interest, the name and contact details of the competent department and, where appointed, the name of the data protection officer or the person responsible for information rights.	Quarterly	Previous state to be erased	Head of the Rector's Office
10.	The results of the collection of statistical data on the activities of the body having public service functions, based on legislation, and changes over time.	Quarterly	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
11.	Mandatory statistical reporting of data of public interest for a particular body.	Quarterly	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
12.	List of contracts for the exploitation of data of public interest to which the body having public service functions is a contracting party.	Quarterly	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
13.	General contractual conditions for the use and exploitation of data of public interest held by the body having public service functions.	Immediately after the changes	Keeping the previous state in the archive for 1 year	Head of the Rector's Office
14.	Special and specific disclosure list for the body having public service functions.	Immediately after the changes	Previous state to be erased	Head of the Rector's Office

III. Management data

Data		Update	Storage	Data source
l.	The annual budget of the body having public service functions, its accounts under the Accounting Act or its annual budget report	Immediately after the changes	For 10 years after the disclosure.	Head of the Rector's Office
2.	Aggregated data on the number of employees and their allowances in the body having public service functions and aggregated data on the salaries, wages and regular allowances and reimbursements of managers and senior officials, and the type and level of allowances granted to other staff	Quarterly	By archiving it for the period provided for by specific legislation, but not less than 1 year	Head of the Rector's Office

3.	Information on the names of the beneficiaries of budget aid granted by the body having public service functions in accordance with the Act on the General Government, the purpose of the aid, the amount of the aid and the place where the aid scheme is implemented, unless the budget support is withdrawn or abandoned by the beneficiary before disclosure.	Until the sixtieth day following the date of the decision	For 5 years after the disclosure	Head of the Rector's Office
4.	Name of contracts related to the use of general government funds and the management of property related to the general government with a value of HUF 5 million or more for the purchase of goods, construction works, services, sale of property, use of property, transfer of property or rights of property value and concession, (type), subject matter thereof, names of the parties to the contract, value of the contract, duration of the contract in the case of a fixed-term contract and changes to the above data, data on procurements directly related to national security or defence interests, and except for classified data. The value of the contract is understood to be the consideration agreed for the subject of the contract, excluding VAT, and in the case of a free transaction, the higher of the market value or the book value of the property. In the case of recurring contracts of a duration of more than one year, the value must be calculated on the basis of the amount of the consideration for one year. The value of contracts concluded with the same contractor and having the same subject matter in the same financial year shall be counted together	Until the sixtieth day following the date of the decision	For 5 years after the disclosure	Head of the Rector's Office
5.	Public data as defined in the Act on Concessions (tender notices, details of tenderers, memos of evaluation, tender results).	Quarterly	By archiving it for the period provided for by specific legislation, but not less than 1 year	Head of the Rector's Office

6.	Payments exceeding HUF 5 million made by a body having public service functions for the performance of its non-core tasks (in particular, support for associations, professional and employee representative bodies of its employees, support for organisations supporting the educational, cultural, social and sports activities of its employees and staff, payments in connection with tasks performed by foundations)	Quarterly	By archiving it for the period provided for by specific legislation, but not less than 1 year	Head of the Rector's Office
7.	Description of the developments supported by the European Union and the contracts relating thereto	Quarterly	By keeping it in the archive for at least 1year	Head of the Rector's Office
8.	Public procurement information (annual plan, summary of the evaluation of tenders, contracts concluded)	Quarterly	By keeping it in the archive for at least 1year	Head of the Rector's Office

Annex 8

REQUEST FOR THE DISCLOSURE OF DATA OF PUBLIC INTEREST (*To be completed in duplicate*!)				
1.	Nature of initiative (to be underlined):	new disclosure	amendment	erasure
2.	Title of the material to be disclosed:			
3.	Reason for disclosure:			
4.	Place of disclosure:			
5.	Provision concerning other data placed on the website (with an exact indication of the data to be amended or erased):			
6.	Name of the attached data files:			
7.	Other provision related to the disclosure:			
8.	Name, title, telephone number, e-mail address of the controller:			
Dated:				

.....

applicant