

PRIVACY NOTICE
for applicants and students
Applicable from: 17 February 2025 until further notice

1. Purpose of Data Processing

The purpose of this Privacy Notice is to inform you about the data processing operations carried out by Dennis Gabor University (registered office: 70 Fejér Lipót Street, Budapest 1119, Hungary) (hereinafter: DGU or the Data Controller) in connection with its core educational activities, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), and the provisions of applicable Hungarian legislation.

A higher education institution's core educational activities include higher education vocational training, bachelor's programmes, master's programmes, and postgraduate specialist training programmes.

2. Data Controller

DGU qualifies as the **Data Controller** with respect to the data processing operations described in this Privacy Notice. The Data Controller's contact details are as follows:

Name of the Data Controller: **Dennis Gabor University**
Registered office: 0 Fejér Lipót Street, Budapest 1119, Hungary
Institutional identifier: FI54333 Telefonszám: +36 20 999 8900
Website: www.gde.hu

Data Protection Officer (DPO) of the University: **dr. Vámos Ágnes**
Contact: adatvedelem@gde.hu

During its data processing operations, the Data Controller complies with the requirements of applicable legislation, and, when establishing its data processing practices, fully respects the protection of individuals' fundamental rights and privacy, with particular regard to the provisions of the General Data Protection Regulation (GDPR).

If you have any questions or comments, please contact us at adatvedelem@gde.hu

3. Data processing related to the student status

The categories of personal data to be processed as defined in **Annex 3 to Act CCIV of 2011 on National Higher Education** (hereinafter: the **NHEA**) are set out in **Annex 1** to this Privacy Notice.



Purpose Of Data Processing	Legal Basis For Data Processing	Personal Data Processed	Duration Of Data Processing
Ensuring that the admissions procedure is conducted in compliance with the applicable legislation.	Legal basis: Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: personal data specified in Section 18(1)(a) of the NHEA.	Personal data specified in Annex 3, Section I/B, point 1(a) of the NHEA.	Eighty years from the date of the termination of the student status. If, as a result of the admissions procedure, no student status is established, the Data Controller shall process the personal data related to the admission for two years from the end of the enrolment period following the given admission period.
Maintaining records required by law, and processing data in the electronic study administration system. For the purpose of performing its statutory record-keeping obligations, the Data Controller operates a unified electronic study administration system.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 18(1)(e); Nftv.Vhr., Section 34.	Personal data specified in Annex 3 under Section I/B of the NHEA, and in Section 60 of the Nftv.Vhr.	Eighty years from the date of the termination of the student status.
Ensuring the proper operation of the institution, organising education and research, and enabling students to exercise their rights and fulfil their obligations.	Legal basis: Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 18(1)(a)–(c) and (f); Annex 2, Section II of the NHEA.	Personal data specified in Annex 3 under Section I/B of the NHEA, and the date of participation in fire safety training.	Eighty years from the date of the termination of the student status. NHEA, Section 18(1)(a)–(c) and (f).
Data processed in connection with the processing operations set out in the Student Requirements System, the Code of Ethics, the House Rules, the IT Security Policy, the Intellectual Property Management Policy, and the Data Controller's Organisational and Operational Regulations (hereinafter: the OOR).	Legal basis: Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 18(1)(a)–(c) and (f).	n particular, but not limited to: the user name required for using the Neptun system (e.g. Neptun code), the initial login password, data generated in the course of using the systems, and data provided by the student or otherwise generated in connection with the assessment of student requests and	Eighty years from the date of the termination of the student status. NHEA, Section 18(1)(a)–(c) and (f). Participation-related data specified in Annex 2, Section II of the NHEA shall be processed until the completion of the programme, while data necessary for compliance with tax and accounting

		requests for legal remedy; data provided by the student or otherwise generated in the course of conducting ethics proceedings; data generated in connection with library use; data related to the use of language programmes; data related to membership of the Student Union (HÖK); data relating to accommodation services; data included in certificates issued at the student's request or with the student's approval.	obligations shall be processed for up to eight years.
Processing data related to student benefits, and assessing and determining eligibility for allowances granted under applicable legislation and the OOR.	In the case of benefits granted to the student on the basis of legislation, processing is necessary for compliance with a legal obligation under Article 6(1)(c) of the GDPR; as regards any special category (health) data strictly necessary for the assessment of the application, Article 9(2)(b) and (f) of the GDPR applies. In the case of benefits provided within the Data Controller's institutional competence, processing is carried out on the basis of the data subject's consent pursuant to Article 6(1)(a) of the GDPR. The assessment and determination of eligibility for allowances granted	Data related to student benefits and allowances, and data necessary for assessing eligibility for benefits and allowances (social circumstances, parents' data, data relating to maintenance/support) Data specified in the OOR that are necessary for awarding institutional scholarships.	Eighty years from the date of the termination of the student status.

	under the Data Controller's OOR is necessary for compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR: NHEA, Section 18(1)(f).		
Processing necessary for the delivery of online distance learning, distance education, and examinations.	Legal basis: Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 18(1)(c).	Name, e-mail address, Neptun code, image and voice; during practical classes, where the masking (background-blurring) function is not used, the student's surroundings; during examinations, an image of the identification document presented for the purposes of identity verification; in the case of a registered student with special educational needs, the personal data of their support person.	With the exception of image and audio recordings – which are stored only if they are recorded – eighty years from the date of the termination of the student status.
Student representation in the committees operating at DGU as set out in the OOR.	On the basis of Section 12(5) of the NHEA, the data subject's consent. If consent to the processing of personal data is withdrawn, the membership (delegate) mandate shall be revoked.	Name, e-mail address, Neptun code.	Eighty years from the date of the termination of the student status.
Supporting the integration and progress of students living with disabilities, and providing allowances by the Social and Equal Opportunities Committee. In the context of this processing, the processing of special category data is unavoidable.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 43(1), Section 49(8), and Section 54. As regards any special category (health) data strictly necessary for assessing the	Personal data specified in Annex 3, Section I/B, point (bh) of the NHEA.	Eighty years from the date of the termination of the student status.

	application, Article 9(2)(b) and (f) of the GDPR applies.		
Organising the professional placement and supporting the completion of the student's professional placement.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: Government Decree No. 230/2012 (VIII. 28.) on certain issues of higher education vocational training and professional placements related to higher education programmes, Section 14	Name, programme name and study schedule, Neptun code, contact details (e-mail address, telephone number).	Eighty years from the date of the termination of the student status.
Alumni career tracking.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: Government Decree No. 230/2012 (VIII. 28.) on certain issues of higher education vocational training and professional placements related to higher education programmes, Section 14	Neptun code, name, sex, e-mail address, date of birth, year of graduation, year of commencement, programme name, level of study, training provider, campus, mode of study, form of funding.	Eighty years from the date of the termination of the student status.
Sending informational e-mails related to studies.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Data Controller is subject: NHEA, Section 18(1)(g).	Neptun code, name, e-mail address, year of commencement, programme name, level of study, training provider, campus, mode of study, form of funding.	Eighty years from the date of the termination of the student status.
Individual career counselling.	Article 6(1)(a) of the GDPR – the data subject's consent.	Name, e-mail address, Neptun code, full-time/part-time, how the student learned about distance education, nature of interest, CV;	The Data Controller shall process the data provided upon applying for counselling and the data generated during the counselling until the end of

		related correspondence; expert comments, date of the counselling session.	the semester in progress at the time of the counselling session.
--	--	---	--

3.1. Data transfers

On the basis of Annex 3, Section I/B, point 4 of the NHEA, the Data Controller transfers personal data as follows: all data to the maintainer; the data necessary for deciding the specific case to the court, the police, the public prosecutor's office, the judicial enforcement officer, and the public administration authority; all data to the national security service to the extent necessary for the performance of its tasks as defined in the law; all data to the body responsible for operating the higher education information system; and, in relation to the programme and the student status, to the body responsible for maintaining records of compliance with the conditions of the Hungarian State Scholarship.

3.2. Access to data, storage, processors

The Data Controller takes particular care to ensure that applicants' and students' data may be accessed, on the part of the Data Controller, only by authorised employees and agents of organisational units involved in organising, delivering and monitoring education, ensuring compliance with study-related and payment obligations, administering and assessing student matters, mandatory data reporting, and professional placements. Accordingly, in particular, study-related data are accessible to the staff member responsible for educational administration and the lecturer of the programme within which the student pursues their studies, while data related to the administration of student matters are managed by the Study Centre. As regards data stored in the Neptun system, both the IT function and the Study Centre have access.

In procedures required to assess the special treatment granted to persons living with disabilities, the Equal Opportunities Coordinator, the Equal Opportunities and Social Committee, and, in the event of a legal remedy, the Appeals Committee, have access to the data.

For the primary storage of personal data, the Data Controller uses the Neptun system, which is uniformly applied in higher education and is operated, as a data processor, by SDA Informatika Zrt. The processing activities of SDA Informatika Zrt. are governed by the data processing agreement concluded with the Data Controller.

Depending on the type of matter and the nature of the data, the Data Controller also stores the data in its other electronic systems.

For the registration of documents related to equal opportunities procedures, the Data Controller's central document management system is used, with access rights granted to the Equal Opportunities Coordinator. Paper-based data are stored at the Data Controller's training locations under secure conditions. For the purposes of secure access control, the porter service operating at the relevant training locations also stores the name and programme data of persons who have attended fire safety training.

Paper-based data are stored at the Data Controller's training locations under secure conditions.

Data Processor	Function
SDA Informatika Zrt. egistered office: 2030 Érd, Retyezáti utca 46. company registration number: 01-10-140314	operation of the Neptun system, used as a unified study administration system in higher education for the primary storage of personal data

4. Confidentiality and security of data

The Data Controller processes personal data confidentially and takes all IT and other measures related to storage and processing that facilitate secure data handling in order to safeguard the data.

Taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, and the risks of varying likelihood and severity to the rights and freedoms of natural persons, the Data Controller and the data processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In the course of providing the service, the Data Controller selects and operates the IT tools used for processing personal data in such a way that the processed data:

- are accessible only to authorised persons;
- are protected against unauthorised access by means of server-level and application-level protection procedures, and the integrity of the data and the verifiability of amendments are ensured;
- remain available throughout the entire duration of the processing.

5. Your rights

Please note that you may exercise your rights granted to you by law by contacting us at adatvedelem@gde.hu.

Pursuant to Article 7(3) of the GDPR, the data subject has the right to withdraw their consent at any time.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Pursuant to Article 15 of the GDPR, the data subject may request access to personal data concerning them as follows.

The data subject has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning them are being processed and, where that is the case, access to the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the right to request from the Data Controller rectification or erasure of personal data concerning the data subject, or restriction of processing, and to object to such processing;
- f) the right to lodge a complaint with a supervisory authority;
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Data Controller shall provide the data subject with a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless the data subject requests otherwise.

Pursuant to Article 16 of the GDPR, the data subject has the right to obtain from the Data Controller rectification of inaccurate personal data concerning them.

Upon the data subject's request, the Data Controller shall, without undue delay, rectify inaccurate personal data concerning the data subject. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Pursuant to Article 17 of the GDPR, the data subject has the right to obtain from the Data Controller the erasure of personal data concerning them as follows.

The data subject has the right to obtain from the Data Controller the erasure of personal data concerning them, and the Data Controller shall be obliged to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject objects to the processing carried out for the performance of a task carried out in the public interest, for the exercise of official authority, or for the legitimate interests of the Data Controller (or a third party), and there are no overriding legitimate grounds for the processing; or the data subject objects to processing for direct marketing purposes;
- c) the personal data have been processed unlawfully;
- d) the personal data have to be erased for compliance with a legal obligation under Union or Member State law (Hungarian law) to which the Data Controller is subject.

Where the Data Controller has made the personal data public and is obliged to erase them, the Data Controller shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform other controllers processing the data that the data subject has requested the erasure by such controllers of any links to, or copies or replications of, those personal data.

The restriction of the data subject's right to erasure may take place only where one of the following exceptions under the GDPR applies; in such cases, further retention of the personal data may be lawful:

- a) for exercising the right of freedom of expression and information, or for compliance with a legal obligation;
- b) for the performance of a task carried out in the public interest;
- c) for the exercise of official authority vested in the Data Controller, or for reasons of public interest in the area of public health;
- d) for archiving purposes in the public interest;
- e) for scientific or historical research purposes or statistical purposes; or
- f) for the establishment, exercise or defence of legal claims.

Pursuant to Article 18 of the GDPR, the data subject has the right to obtain from the Data Controller restriction of processing concerning them as follows.

The data subject has the right to obtain restriction of processing where one of the following applies:

- a) the data subject contests the accuracy of the personal data, for a period enabling the Data Controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- d) the data subject has objected to processing carried out for the performance of a task carried out in the public interest, for the exercise of official authority, or for the legitimate interests of the Data Controller (or a third party);
- e) in such a case, the restriction shall apply pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.

Where processing has been restricted in accordance with the above, 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.

Pursuant to Article 20 of the GDPR, the data subject has the right to data portability as follows:

The data subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on the data subject's consent or on a contract, and the processing is carried out by automated means.

In exercising the right to data portability, the data subject has the right, where technically feasible, to have the personal data transmitted directly from one controller to another.

The exercise of the right to data portability shall be without prejudice to the right to erasure. The right to data portability shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

Pursuant to Article 21 of the GDPR, the data subject has the right to object to the processing of personal data concerning them as follows:

The data subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on points (e) or (f) of Article 6(1) of the GDPR, including profiling based on those provisions. In such a case, the Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

6. Remedies before the courts, complaint to the Supervisory Authority, questions

If the data subject considers that, in the course of processing their personal data, the Data Controller has infringed the applicable data protection provisions, then:

- they may lodge a complaint with the National Authority for Data Protection and Freedom of Information (address: 9-11 Falk Miksa Street, Budapest 1055, Hungary; postal address: 1363 Budapest, Pf.: 9), or
- they may apply to the court in order to protect their personal data.

In the event of court proceedings, you may choose whether to bring your claim before the competent court having jurisdiction based on your place of residence or habitual residence, or the registered office of the Data Controller.

We kindly ask data subjects that, if they consider that an infringement has occurred or is occurring in relation to any of the processing operations described in this Notice, they should, where possible, first contact the University's Data Protection Officer at adatvedelem@gde.hu. The University will take all necessary steps to ensure that complaints are investigated thoroughly and that the matter is resolved in a manner that is satisfactory for all parties concerned.

Annex 1

Personal data processed by the Data Controller under the NHEA

1. Data recorded pursuant to the NHEA

a) Data related to admission:

aa) the applicant's family name and given name(s), sex, facial image, birth family name and given name(s), mother's birth family name and given name(s), place and date of birth, nationality, permanent address, place of stay, correspondence address, email address and other contact details, telephone number, education identification number, type, number and validity of identity document, tax identification number, social security identification number, digital citizen identifier; in the case of non-Hungarian citizens, the legal basis for staying in Hungary and the document authorising the stay – and, pursuant to a separate law, in the case of persons entitled to the right of free movement and residence, the document certifying the right of residence – the "Hungarian Card", "Hungarian Relative Card", and the details of the international insurance document;

ab) data relating to the school-leaving examination (matura);

ac) data relating to the secondary school;

ad) data necessary for assessing the admission application;

ae) data relating to the admission procedure; the admission identifier;

af) the identification number of the declaration pursuant to Section 48/D(2).

b) Data related to student status:

ba) the student's name, sex, birth name, mother's name, place and date of birth, nationality, permanent address, place of stay, correspondence address and telephone number, email address; in the case of non-Hungarian citizens, the legal basis for staying in Hungary and the designation and number of the document authorising the stay – and, pursuant to a separate law, in the case of persons entitled to the right of free movement and residence, the document certifying the right of residence;

bb) the type of student (visiting student) status; the date and manner of its commencement and termination; the name of the programme pursued by the student; whether it is state-funded and the mode of study; the expected date of completion; assessment of the student's studies, examination data, semesters commenced, utilised support period, and suspension of student status;

bc) the place and period of partial studies undertaken in foreign higher education;

bd) credits obtained and recognised during the programme; studies credited/recognised;

be) data relating to student benefits; data required to assess eligibility for benefits (social situation, parents' data, maintenance/support-related data);

bf) data relating to student employment/work;

bg) data relating to student disciplinary and compensation/liability matters;

bh) data required to assess eligibility for special treatment for persons with disabilities;

- bi)* data relating to student accidents;
- bj)* the serial number of the student card; the identification number of the master record (registry sheet);
- bk)* the student's education identification number; identity document number; photograph; social security identification number;
- bl)* the electronic copy of the thesis (dissertation) and the diploma supplement; data relating to completion of practical placement, the absolutorium (certificate of completion of studies), the final examination (doctoral defence), the language examination, as well as data relating to the degree certificate, diploma supplement and the micro-credential;
- bm)* data necessary for the performance of rights and obligations arising from student status.
- c)* data relating to graduate career tracking;
- d)* the student's tax identification number;
- e)* data serving to identify the documents evidencing the data;
- f)* data relating to fees and charges paid by the student – including instalment facilities, deferral and exemption associated with the obligation;
- g)* where student or housing support is granted on the grounds of receiving infant care allowance, childcare assistance benefit, child-raising support, childcare benefit, regular child protection support, or due to disadvantaged status: data relating to these fees/benefits/supports;
- h)* data relating to scholarships disbursed with regard to the student's status in order to support the student's studies – established by Government decree in accordance with Section 85(1) and (2);
- i)* data relating to student competence assessment and its results;
- j)* data relating to the existence and type of a loan granted by the Student Loan Centre (Diákhitel Központ), and, in the case of a restricted-use loan, the amount of the student loan requested by the student, the loan agreement number, the amount transferred to the higher education institution and the date of the transfer;
- k)* the date and reason for removal from the personal data and address register.

2. Purpose of processing

As set out in Section 18(1). The higher education institution may process personal data and special categories of personal data only in connection with the legal relationship (student status), and with establishing and fulfilling benefits, discounts and obligations, for national security reasons, and for the purposes of managing the registers defined in this Act, to the extent necessary and in a purpose-limited manner.

3. Retention period

For eighty (80) years from the notification of the termination of student status.

4. Conditions for data transfer

The data may be transferred to:

- a) the maintainer (operator/founding body): all data, for the performance of tasks related to the maintainer's governance/management;
- b) the court, police, public prosecutor's office, judicial enforcement officer, and administrative authority: data necessary to decide the specific case;
- c) the national security service: all data necessary to perform the tasks defined in the Nbtv.;
- d) the body responsible for operating the higher education information system: all data;
- e) -;
- f) the body responsible for keeping records of compliance with the conditions of the Hungarian state scholarship: data relating to the programme and the student status.

5. Additional retention for specific data

The higher education institution records data relating to the student's marital status and status as a student with children for ten (10) years from the notification of the termination of student status, for the purpose of determining the support period under the Hungarian state scholarship.

Personal data and special categories of personal data recorded and processed by the maintainer of the higher education institution

1. Data recorded pursuant to the Nftv.

The maintainer of the higher education institution processes the personal data and special categories of personal data that are, on the basis of points I/A.4 and I/B.4, transferred individually, or via its IT system, and/or made directly accessible by the higher education institution to the maintainer for the purpose of performing tasks related to maintainer governance and exercising maintainer rights.

2. Retention period

For five (5) years from the date of transfer.

3. Further transfers of the data listed in point 1

The data may be transferred to: the court, police, public prosecutor's office, judicial enforcement officer, and administrative authority (data necessary to decide the specific case); persons/authorities entitled to verify compliance with rules relating to work (employment-related data); the national security service (all data necessary to perform tasks defined in the Nbtv.); the Student Loan Centre (data related to the lawful disbursement of student loans and the continuation of studies); and, pursuant to Section 28 of Avtv2, to the applicant for the purpose of fulfilling a request for access addressed to the maintainer, limited to data qualifying as data of public interest by virtue of being publicly available in the public interest under Section 26(3) of Avtv2.