17. Data Protection and Data Management Policy (DPDMP 2019)[1]

unanimously adopted by the Senate of the Dharma Gate Buddhist College
within the framework laid down by 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 Directive 95/46/EC (General Data Protection Regulation – hereinafter: GDPR), as well as by Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Infotv.),
having regard to the provisions of Act CCIV of 2011 on National Higher Education (hereinafter: NHEA), Government Decree 87/2015 (IV. 9.) on the implementation of certain provisions of Act CCIV of 2011 on National Higher Education (hereinafter: NHEA Decree), Act LXXXIX of 2018 on Educational Records (hereinafter: Onytv.), Government Decree 423/2012 (XII. 29.) on Admission to Higher Education (Ffer.), Government Decree 24/2013 (II. 5.) on National Higher Education Excellence (Nfkr.), Government Decree 19/2012 (II. 22.) on Certain Issues of Quality Assessment and Quality Enhancement in Higher Education (Fmfr.), as well as Act I of 2012 on the Labour Code (MT) and Act V of 2013 on the Civil Code (hereinafter: Civil Code),
The institutional framework for data processing and transmission at the Dharma Gate Buddhist College is defined as follows:

17.1. General Provisions

17.1.1. Purpose and Scope of the Regulations

17.1.1.1. The purpose of this Policy is to determine – in order to guarantee the right of informational self-determination and the freedom of information, the protection of personal data, and the enforcement of fundamental rules ensuring access to and dissemination of data of public interest and data made public on grounds of public interest – the lawful framework for the recording, management, processing, and transmission of data maintained at the Dharma Gate Buddhist College (hereinafter: the College). It further aims to ensure compliance with requirements of data protection and data security, and to prevent unauthorised access, alteration of data, and unauthorised disclosure.
17.1.1.2. The scope of this Policy extends to all:
a) employees, instructors, researchers and teachers of the College, irrespective of the legal form of their employment;
b) students of the College, irrespective of the form of study;
c) all data processed at the College;
d) all organisational units engaged in data processing; and
e) all data transferred and processed in relation to outsourced taxation and accounting activities carried out by contracted enterprises.
17.1.1.3. This Policy applies equally to data processing and data management carried out by fully or partially automated means, as well as to manual processing.

17.1.2. Definitions

For the purposes of this Policy:
17.1.2.1. ***data subject***: any identified or identifiable natural person based on any information [Infotv. §3(1)];

[1] Adopted by Senate Resolution No. 30/2017. (05.18.) of 18 May 2017. Supplemented by Senate Resolution No. 46/2017. (12.14.) of 14 December 2017. Amended by Senate Resolution No. 43/2019. (09.26.) of 26 September 2019, and, with respect to Annex 4, by Senate Resolution No. 6/2020. (02.27.) of 27 February 2020.

17.1.2.2. ***identifiable natural person***: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [Infotv. §3(1a)];
17.1.2.3. ***personal data***: any information relating to the data subject [Infotv. §3(2)];
17.1.2.4. ***sensitive data***: all data falling into special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, health data and data concerning a natural person's sex life or sexual orientation [Infotv. §3(3)];
17.1.2.5. ***genetic data***: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that person and which result, in particular, from an analysis of a biological sample from the natural person in question [Infotv. §3(3a)];
17.1.2.6. ***biometric data***: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [Infotv. §3(3b)];
17.1.2.7. ***health data***: personal data related to the physical or mental health of a natural person, including data concerning health care services provided to that person, which reveal information about his or her health status [Infotv. §3(3c)];
17.1.2.8. ***criminal personal data***: personal data relating to a criminal offence or criminal proceedings, generated by or held at the authorities empowered to conduct criminal proceedings or investigations, or by the penitentiary system, and which may be linked to the data subject, including data relating to criminal records [Infotv. §3(4)];
17.1.2.9. ***data of public interest***: information or knowledge, recorded in any manner or form, that is not personal data and that is managed by, or relates to the activities of, a body or person performing a State or local government duty, or another public duty prescribed by law, or that arises in connection with the performance of such duty. This includes, in particular, data concerning competence, jurisdiction, organisational structure, professional activity, its effectiveness and evaluation, categories of data held, governing legislation, financial management, and concluded contracts [Infotv. §3(5)];
17.1.2.10. ***data made public on grounds of public interest***: any data not falling under the definition of data of public interest, whose disclosure, accessibility or availability is ordered by law in the public interest [Infotv. §3(6)];
17.1.2.11. ***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 [Infotv. §3(7)];
17.1.2.12 ***data controller***: a natural or legal person, or an organisation without legal personality, which alone or jointly with others determines the purposes of data processing, makes and implements decisions regarding the processing (including the means used), or has them implemented by the processor [Information Act Section 3 (9)].
17.1.2.13. ***joint controller***: a controller who, within the limits set by law or by a binding legal act of the European Union, determines the purposes and means of processing jointly with one or more other controllers, and takes or implements decisions on processing (including the means used) jointly with one or more other controllers or has them implemented by a data processor [Infotv. §3(9a)];
17.1.2.14. ***data processing***: any operation or set of operations performed on data, regardless of the procedure applied, such as collection, recording, organisation, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, blocking, erasure and destruction, as well as preventing further use of the data, making photo, audio or video recordings, and recording physical characteristics suitable for identifying a person (e.g. fingerprint, palm print, DNA sample, iris image) [Infotv. §3(10)];
17.1.2.15. ***data transmission***: making data accessible to a specific third party [Infotv. §3(11)];
17.1.2.16. ***indirect data transmission***: transmission of personal data to a controller or processor engaged in data processing in a third country or international organisation, by means of another controller or processor engaged in data processing in a third country or international organisation [Infotv. §3(11a)];
17.1.2.17. ***international organisation***: an organisation subject to international public law and its subordinate bodies, as well as any other body established by agreement between two or more States or formed on the basis of such agreement [Infotv. §3(11b)];
17.1.2.18. ***disclosure***: making data accessible to anyone [Infotv. §3(12)];
17.1.2.19 ***data erasure***: the rendering of data unrecognisable in such a way that its restoration is no longer possible [Information Act Section 3 (13)].
17.1.2.20. ***restriction of processing***: marking stored data with the aim of limiting its future processing [Infotv. §3(15)];

17.1.2.21. ***destruction of data***: the complete physical destruction of the data carrier containing the data [Infotv. §3(16)];
17.1.2.22. ***data processing operation***: all processing activities carried out by a processor on behalf of, or under the instructions of, the controller [Infotv. §3(17)];
17.1.2.23. ***data processor***: a natural or legal person, or an organisation without legal personality, which – within the limits and conditions set by law or a binding legal act of the European Union – processes personal data on behalf of, or under the instructions of, the controller [Infotv. §3(18)];
17.1.2.24. ***data custodian***: the public body responsible for producing data of public interest that must be published electronically, or in whose operations such data arises [Infotv. §3(19)];
17.1.2.25. ***data publisher***: the public body which – if the data custodian does not publish the data itself – publishes the data provided by the data custodian on its website [Infotv. §3(20)];
17.1.2.26. ***data set***: the totality of data managed in a single register [Infotv. §3(21)];
17.1.2.27. ***third party***: a natural or legal person, or an organisation without legal personality, other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data [Infotv. §3(22)];
17.1.2.28. ***data breach***: a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorised transmission or disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed [Infotv. §3(26)];
17.1.2.29. ***profiling***: any form of automated processing of personal data consisting of the use of personal data to evaluate, analyse or predict personal aspects relating to the data subject, in particular with regard to work performance, economic situation, health, personal preferences or interests, reliability, behaviour, location or movements [Infotv. §3(27)];
17.1.2.30. ***recipient***: a natural or legal person, or an organisation without legal personality, to whom personal data is disclosed by the controller or processor [Infotv. §3(28)];
17.1.2.31. ***pseudonymisation***: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately, and subject to technical and organisational measures ensuring that the data cannot be attributed to an identified or identifiable natural person [Infotv. §3(29)].

17.2. Protection of Personal Data

17.2.1. Data Processing

17.2.1.1 Personal data may be processed (legal basis) only if at least one of the following applies:
A) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
B) 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;
C) processing is necessary for compliance with a legal obligation to which the controller is subject;
D) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
E) 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 controller;
F) processing is necessary for the purposes of the legitimate interests pursued by the controller 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 the protection of personal data, in particular where the data subject is a child. [GDPR Article 6(1)(a)–(f)]
17.2.1.2 The legal basis set out in points C) and E) of 17.2.1.1 is met if
a) a law – or, on the basis of authorisation by law and within the scope defined therein, in the case of data that are not sensitive data or criminal personal data, a local government decree – orders processing for a purpose based on the public interest,
b) in the absence of point a), it is absolutely necessary for the performance of the controller's statutory tasks and the data subject has expressly consented to the processing of the personal data,
c) in the absence of point a), it is necessary and proportionate for the protection of the vital interests of the data subject or another person, and for averting or preventing an imminent danger threatening life, physical integrity or property, or
d) in the absence of point a), the personal data have been made public by the data subject explicitly and the processing is necessary and proportionate for achieving the purpose of the processing. [Infotv. §5(1)]
17.2.1.3 In the case of processing specified in points C) and E) of 17.2.1.1, point a) of 17.2.1.2, and point b) of 17.2.1.4

(hereinafter: mandatory processing), the types of data to be processed, the purpose and conditions of processing, the accessibility of data, the identity of the controller, and the duration of processing or the periodic review of its necessity shall be determined by the law or local government decree ordering the processing. [Infotv. §6(3)] If the duration of mandatory processing or the periodic review of its necessity is not determined by law, by a local government decree, or by a binding legal act of the European Union, the controller shall, at least every three years from the start of processing, review whether the processing of personal data by the controller or by a processor acting on its behalf or under its instructions is necessary to achieve the purpose of the processing. The controller shall document the circumstances and result of this review, retain this documentation for ten years after completion of the review, and, at the request of the National Authority for Data Protection and Freedom of Information (hereinafter: the Authority), make it available to the Authority. [Infotv. §5(5)]

17.2.1.4 Sensitive data

a) may be processed in accordance with points c)–d) of 17.2.1.2, or

b) may be processed if it is absolutely necessary and proportionate for the implementation of an international agreement promulgated by law, or if a law so orders for the enforcement of a fundamental right guaranteed by the Fundamental Law, as well as for reasons of national security, the prevention, detection or prosecution of criminal offences, or for defence interests. [Infotv. §5(2)]

17.2.1.5 The College shall keep records of the personal and sensitive data that are indispensable

a) for the proper operation of the institution,

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

c) are necessary for the organization of education and research,

d) for the exercise of the rights and fulfilment of the obligations of applicants and students,

e) are necessary for maintaining records as defined by legislation,

f) for determining, assessing and certifying eligibility for benefits provided for by law and by the higher education institution's Organizational and Operational Regulations; and

.

[Section 18 (1) of the Act on National Higher Education (NHEA)].

17.2.1.6 The scope of the data kept on the basis of point 17.2.1.5, the purpose and duration of processing, and the conditions for the transmission of the recorded data are set out in Annexes 3 and 6 to the NHEA. The recorded data may be used for statistical purposes and may be transferred to the official statistical service for statistical use. [NHEA §18(2)]

17.2.1.7 The processing of personal or sensitive data not listed in the Act referred to in point 17.2.1.6 may take place on one of the legal bases set out in point 17.2.1.1 and only if the data are necessary for the specific purpose of the processing in question. On the basis of the specific processing purpose, the quantity of personal data collected, the extent of their processing, the duration of their storage and their accessibility must be determined. It must be ensured that, by default, personal data are not made accessible to an indefinite number of persons without the intervention of the data subject. [GDPR Article 25(2)] Data collected may be used for a different purpose only with the data subject's consent or on the basis of a law or a binding legal act of the European Union, unless the different-purpose processing – on the basis of a written assessment carried out before commencing the application of the different purpose and in line with the criteria set out in GDPR Article 6(4)(a)–(e) – is compatible with the purpose for which the personal data were originally collected.

17.2.1.8 For processing not based on a statutory requirement as described in point 17.2.1.7, the controller(s) must notify the Rector, using the designated form (Annex 1), for the purpose of registration at the College. Processing may begin only after written consent has been issued by the Rector. The facts relating to the processing are recorded by the College's system administrator.

17.2.1.9 In order to ensure the data subjects' right to prior information, before commencing the first processing operation carried out by it or by a processor, the College shall publish on its website its privacy notice (and any amendments) that complies with the content requirements set out in the relevant legislation [GDPR Articles 12–14; Infotv. §16]. In addition to the general privacy notice, purpose-specific, individual privacy notices may also be prepared (together: the privacy notice).

17.2.1.10 Where processing is based on consent, the controller must be able to demonstrate that, having been informed by the privacy notice and accepting it, the data subject has voluntarily consented to the processing of the specifically identified personal data. [GDPR Article 7]

17.2.1.11 The data subject has the right, on grounds relating to his or her particular situation, to object at any time to processing of personal data based on points E) or F) of 17.2.1.1, including profiling based on those provisions. In such

a case, the College shall no longer process the personal data unless it demonstrates—by a written legitimate-interest assessment recorded in the controller's register (17.2.8.1)—that there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or that the processing relates to the establishment, exercise or defence of legal claims. [GDPR Article 21]

17.2.1.12 Personal data collected for the purposes of scientific research may be used only for scientific research. The link between the personal data and the data subject must be rendered permanently impossible as soon as the research purpose allows. Until that time, data that can identify a specific or identifiable natural person must be stored separately. Such data may be linked with other data only where necessary for the research purpose. The body or person conducting the research may disclose personal data only if

a) the data subject has consented; or

b) disclosure is necessary to present the results of research conducted on historical events. [Infotv. §5(8)]

17.2.2. Data security and incident handling

17.2.2.1 To ensure an appropriate level of security for the personal data processed and the effective protection of the data subjects' fundamental rights, the controller and the processor shall implement technical and organisational measures proportionate to the risks posed by the processing—particularly the risks associated with processing sensitive data. In designing and implementing these measures, the controller and the processor shall take into account all the circumstances of the processing, in particular the state of the art, the costs of implementation, the nature, scope and purposes of processing, and the varying likelihood and severity of the risks to data subjects' rights (privacy by design and by default). [GDPR Article 25; Infotv. §25/I(1)–(2)]

17.2.2.2 The measures specified in 17.2.2.1 shall ensure:

a) denial of access by unauthorised persons to the tools used for processing (hereinafter: the processing system)

b) prevention of unauthorised reading, copying, modification or removal of data carriers;

c) prevention of unauthorised input of personal data into, and unauthorised access to, modification of or deletion of personal data stored in, the processing system;

d) prevention of the use of processing systems by unauthorised persons via data-transmission equipment;

e) that persons authorised to use the processing system can access only those personal data specified in their access permissions, and that access to sensitive data is granted solely to those whose tasks related to the processing operation make such access strictly necessary;

f) that it is verifiable and ascertainable to which recipient personal data have been, or may be, transmitted via data-transmission equipment, or made, or may be made, available;

g) that it is subsequently verifiable and ascertainable which personal data were entered into the processing system, at what time and by whom;

h) prevention of unauthorised access to, copying, modification or deletion of personal data during their transmission or during the transport of the data carrier;

i) restorability of the processing system in the event of a malfunction; and

j) the operability of the processing system, generation of reports on errors occurring during its operation, and that stored personal data cannot be altered even through incorrect operation of the system;

k) that data processed electronically in different registers—unless permitted by law—are not directly linkable and assignable to the data subject.

[GDPR Article 32; Infotv. §25/I(3)–(4); §5(6)]

17.2.2.3 Persons carrying out processing and processing operations are obliged to keep confidential the personal data they become aware of.

17.2.2.4 In the event of a personal data breach occurring in the course of the College's processing activities, the College shall

a) identify and record the nature of the breach, including—where possible—the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned; [GDPR Article 33(3)(a); Infotv. §25/J(5)(a)]

b) assess and record the likely consequences of the personal data breach; [GDPR Article 33(3)(c); Infotv. §25/J(5)(c)]

c) develop and implement the measures necessary to remedy the personal data breach, including, where applicable, measures to mitigate any possible adverse effects arising from the breach; [GDPR Article 33(3)(d); Infotv. §25/J(5)(d)]

d) notify the Authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural

persons. Where the notification is not made within 72 hours, the reasons for the delay shall be submitted with the notification. [GDPR Article 33(1); Infotv. §25/J(1)–(3)]
f) If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and the conditions in GDPR Article 34(3) do not apply, the College shall inform the data subject of the personal data breach without undue delay. [GDPR Article 34; Infotv. §25/K]
17.2.2.5 Where the personal data breach concerns exclusively the College's activities as a processor, in addition to the measures in points 17.2.2.4 a)–c), the College shall notify the controller of the personal data breach without undue delay after becoming aware of it. [GDPR Article 33(2); Infotv. §25/J(4)]

17.2.3 Adatfeldolgozás

17.2.3.1 The rights and obligations of the processor in connection with the processing of personal data are determined by the controller within the framework of the applicable legislation. The controller is responsible for the lawfulness of the instructions it issues.
17.2.3.2 The processor may use another (sub-)processor in accordance with the controller's instructions, unless authorised to do so by law or a binding legal act of the European Union.
17.2.3.3 The processor may not make substantive decisions regarding the processing, may process the personal data that come to its knowledge solely in accordance with the controller's instructions, may not carry out processing for its own purposes, and is obliged to store and retain personal data in line with the controller's directions.
17.2.3.4 The contract governing processing must be in writing and contain the elements required by EU and Hungarian legislation. The College may engage only such processors as provide sufficient guarantees to implement appropriate technical and organisational measures ensuring GDPR-compliant processing and the protection of data subjects' rights. [GDPR Article 28; Infotv. §§25/C–25/D]

17.2.4. Linking of data

17.2.4.1 The data defined by the legislation referred to in point 17.2.1.5 and processed by individual organisational units may be linked within the College where necessary. They may be linked with data held by another controller only where duly justified and only if the data subject has consented or the law permits it, and if the conditions for processing are met for each item of personal data.
17.2.4.2 The facts concerning the linking of processing operations must be notified by the controller(s) initiating the linking to the Rector for registration at the College using the designated form (Annex 2). Implementation of the data linking is conditional upon the issuance of written consent by the Rector. The facts concerning the data linking are recorded by the College's system administrator.
17.2.4.3 To protect datasets processed electronically in different registers, an appropriate technical solution must ensure that—unless permitted by law—the data stored in the registers are not directly linkable and assignable to the data subject.

17.2.5. Disclosure of personal data

17.2.5.1 The disclosure of personal data processed at the College is prohibited, unless ordered by law.
17.2.5.2 Students' grades, examination results, and the fact of whether or not they have received any monetary support constitute personal data. In the event of disclosure—except for nominations for the National Higher Education Scholarship as included in a Senate decision—codes (e.g. Neptun code) must be used instead of names.

17.2.6. Data transmission

17.2.6.1 The data defined by the legislation referred to in point 17.2.1.5 and processed by the organisational units of the College may be transmitted to another competent organisational unit of the College to the extent and for the duration necessary for performing administrative and organisational tasks related to employment, other work-related legal relationships, or student status. On the basis of statutory authorisation, employee data may be transmitted to the Maintainer to the extent necessary for exercising maintainer's rights, and student data to the extent necessary for performing tasks related to maintainer oversight, as well as certain data to authorities, courts and State bodies for the purposes and within the scope defined by law. [NHEA Annex 3, points I/A.4 and I/B.4]
17.2.6.2 In cases not covered by point 17.2.6.1, processing related to intra-College data transmission must be notified to the Rector using the designated form (Annex 3). Implementation of the data transmission is conditional upon the

issuance of written consent by the Rector. The facts concerning the data transmission are recorded by the College's system administrator.
17.2.6.3 Requests from bodies or persons outside the College for the provision of data—except for mandatory data provision to the higher education information system [NHEA §19(3)]—may be fulfilled only if the conditions set out in point 17.2.6.4 are met.
17.2.6.4 Data processed at the College—apart from the cases defined in point 17.2.6.1—may be transmitted only if the data subject has given written consent or the law permits it, and if the College has verified that the conditions for processing are met for each item of personal data. The data subject may also grant such authorisation in advance, specifying a period, a defined circle of requesting bodies, and the scope of the data to be transmitted.
17.2.6.5 In the case of lawful data provision without personal consent as set out in points 17.2.6.1 and 17.2.6.4, the competent controller or processor shall inform the Rector—directly or through their superior—on a quarterly basis.
17.2.6.6 In the case of an external request, data transmission—except for the statutory exceptions in points 17.2.6.1 and 17.2.6.4—must be notified to the Rector using the designated form (Annex 3). Implementation of the data transmission is conditional upon the issuance of written consent by the Rector. The facts concerning the data transmission are recorded by the College's system administrator.
17.2.6.7 Pursuant to §146 of Government Decree 451/2016 (XII. 19.) on detailed rules of electronic administration, the College is a public body designated for cooperation under Part Three of Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services. Therefore, as of 1 January 2018, the College conducts outgoing and incoming data transmissions performed as a cooperating body falling under paragraph (1)—including the transmission of documents required by law—using the Office Gate mailbox service. The rules governing data and document transmission via the Office Gate are set out in DGBC's Information Transfer Policy, which is issued and amended by the Rector in the form and with the content conforming to the model policy published by the authority supervising electronic administration at State level.[2]
17.2.6.8 The Rector designates the Office Gate contact person, the case officers, and the persons holding the types of electronic signatures required by law..[3]

17.2.7. Data transmission abroad

17.2.7.1 Personal data may be transmitted to a controller engaged in processing in a non-EEA State, or handed over to a processor carrying out processing in a third country or within an international organisation, if
a) the data subject has given explicit consent; or
b) the international data transmission is necessary to achieve the purpose of the processing, and
ba) the conditions laid down in Infotv. §5 are met during the transmission, and
bb) an adequate level of protection is ensured for the personal data transmitted in respect of the controller or processor engaged in processing in the third country or within the international organisation; or
c) the international data transmission is necessary in the exceptional cases defined in Infotv. §11.

17.2.7.2 An adequate level of protection for personal data is ensured if
a) it is established by a binding legal act of the European Union,
b) there is an international agreement in force between the third country and Hungary containing safeguard rules on enforcing the rights of data subjects set out in Infotv. §14, on ensuring the right to a remedy, and on independent supervision of processing and/or processing operations; or
c) processing and/or processing operations are carried out in accordance with binding organisational rules.
17.2.7.3 Personal data may be transferred to a third country for the purpose, under the conditions, and within the scope of data defined in an international treaty on mutual legal assistance, exchange of tax information, or the avoidance of double taxation – even in the absence of the conditions set out in point 17.2.7.2.
17.2.7.4 A data transfer shall be regarded as equivalent to a domestic transfer within the territory of Hungary if the country concerned is a Member State of the European Union, or a state party to the Agreement on the European Economic Area, or a state whose nationals, under an international treaty concluded between the European Union and its Member States and a state not party to the EEA Agreement, enjoy the same status as the nationals of an EEA state (EEA state).

---

[2] Chapter 17.2.6 was supplemented with point 17.2.6.7 by Senate Resolution No. 46/2017. (12.14.) of 14 December 2017. The DGBC Information Transfer Regulations were issued by Rector's Instruction No. 4/2017. (12.14.).

[3] Chapter 17.2.6 was supplemented with point 17.2.6.8 by Senate Resolution No. 46/2017. (12.14.) of 14 December 2017.

17.2.7.5 Otherwise, the rules governing domestic data transfers shall apply to transfers abroad (data subject's consent, prior authorisation by the Rector, registration by the system administrator).

17.2.8. Data Protection Records

17.2.8.1 The College, as data controller, shall maintain records (hereinafter together: controller's records) of the processing of personal data under its management, of data breaches, and of measures taken in relation to the data subject's right of access. The controller's records shall include:
a) the name and contact details of the data controller, including any joint controllers, and the Data Protection Officer,
b) the purpose or purposes of the processing,
c) in the case of data transfers or planned transfers, the categories of recipients – including third-country recipients and international organisations,
d) the categories of data subjects and of the data processed,
e) if profiling is applied, a statement of that fact,
f) in the case of international transfers, the categories of data transferred,
g) the legal grounds of the processing operations – including transfers,
h) where known, the date of deletion of the processed personal data,
i) a general description of the technical and organisational security measures carried out under this Act,
j) the circumstances of any data breaches related to the data it manages, their effects, and the measures taken to address them,
k) the legal and factual grounds of any measure taken under this Act to restrict or deny the enforcement of the data subject's right of access [GDPR Article 30(1); Infotv. Section 25/E(1)].
17.2.8.2 The College, as data processor, shall maintain records (hereinafter: processor's records) of the data processing it carries out on behalf of, or under the instructions of, individual controllers. The processor's records shall include:
a) the name and contact details of the controller, the processor, any additional processors, and the processor's Data Protection Officer,
b) the types of processing carried out on behalf of or under the instructions of the controller,
c) in the case of international transfers carried out at the explicit instruction of the controller, the fact of the transfer and the identification of the recipient third country or international organisation,
d) a general description of the technical and organisational security measures applied [GDPR Article 30(2); Infotv. Section 25/E(2)].
17.2.8.3 The controller's and processor's records shall be maintained by the system administrator in written or electronically recorded form and, upon request, made available to the Authority [GDPR Article 30(3)–(4); Infotv. Section 25/E(3)].
17.2.8.4 For the purpose of ensuring the verifiability of the lawfulness of processing operations carried out electronically on personal data, the College shall record in an automated data processing system operated by the system administrator (hereinafter: electronic log):
a) the definition of the categories of personal data affected by the processing operation,
b) the purpose and justification of the processing operation,
c) the exact time when the processing operation was carried out,
d) the identification of the person performing the processing operation,
e) in the case of data transfers, the recipient of the transfer [Infotv. Section 25/F(1)].
17.2.8.5 Data recorded in the electronic log may be accessed and used solely for the purposes of verifying the lawfulness of processing, enforcing data security requirements, and conducting criminal proceedings. The College, through the system administrator, shall provide access to the log and transfer data from it to the Authority or to any person or body carrying out activities defined by law, upon their request [Infotv. Section 25/F(2)–(3)].
17.2.8.6 Data recorded in the controller's and processor's records and in the electronic log shall be retained for ten years following the deletion of the processed data [Infotv. Section 25/F(4)].

17.2.9. Rights of Data Subjects and their Enforcement

17.2.9.1 The data subject shall have the right, in relation to personal data processed by the controller or by a processor acting on its behalf or under its instructions, under the conditions set out in the Infotv., to:
a) receive information on facts related to the processing prior to the commencement of the processing (right to prior information [GDPR Articles 13–14; Infotv. Section 16]),

b) obtain, upon request, their personal data and information related to their processing from the controller (right of access [GDPR Article 15; Infotv. Section 17]),
c) request the controller to rectify or complete their personal data, either upon request or in other cases specified in this chapter (right to rectification [GDPR Article 16; Infotv. Section 18]),
d) request the controller to restrict the processing of their personal data, either upon request or in other cases specified in this chapter (right to restriction of processing [GDPR Article 18; Infotv. Section 19]),
e) request the controller to delete their personal data in the cases specified in this chapter and in Chapter II/A of the Infotv. (right to erasure / right to be forgotten [GDPR Article 17; Infotv. Section 20(e)]).
17.2.9.2 Upon the data subject's request, the controller shall provide, within the shortest possible time but no later than 25 days from the submission of the request, clear and intelligible information in writing, if so requested, on the data processed by it or by a processor engaged on its behalf or under its instructions, the source of the data, the purpose, legal basis, and duration of the processing, the name and address of the processor and its activities related to processing, the circumstances, effects, and measures taken to address a data breach, and – in the case of transfers of the data subject's personal data – the legal basis and the recipient of the transfer [Infotv. Section 15(1)].
17.2.9.3 The information under point 17.2.9.2 shall be free of charge if the requesting party has not yet submitted a request for information regarding the same category of data to the controller in the current year. In other cases, reimbursement of costs may be charged. The amount of reimbursement may also be determined in the contract concluded between the parties. Any reimbursement already paid shall be refunded if the data were processed unlawfully or if the request for information resulted in rectification [Infotv. Section 15(3)].
17.2.9.4 The controller may refuse to provide the data subject with information only in the cases defined in Section 9(1) and Section 19 of the Infotv. (restriction of processing). In the case of refusal, the controller shall inform the data subject in writing of the legal provision under which the refusal was made.
17.2.9.5 If processed personal data are inaccurate, incorrect, or incomplete, and the correct data are available to the controller, the controller shall, in particular at the request of the data subject, promptly correct or rectify the personal data [Infotv. Section 18].
17.2.9.6 Personal data shall be deleted if:
a) the processing is unlawful, in particular if the processing:
aa) is contrary to the principles set out in Section 4 of the Infotv.,
ab) its purpose has ceased, or further processing is no longer necessary to achieve its purpose,
ac) the time limit set by law, international treaty, or binding legal act of the European Union has expired, or
ad) its legal basis has ceased and there is no other legal basis for processing,
b) the data subject withdraws their consent to the processing or requests the deletion of their personal data, except where the processing is based on point 17.2.1.1(a) or (c) or Section 17.2.1.3(b),
c) deletion of the data has been ordered by law, an EU legal act, the Authority, or a court, or
d) the period of restriction of processing (Infotv. Section 19(1)(b)–(d)) has expired.
17.2.9.7 In the cases defined in points 17.2.9.6(ab) and (ac), the obligation to delete shall not apply to personal data whose carrier must be placed under archival custody pursuant to legislation on the protection of archival material.
17.2.9.8 Instead of deletion, the controller shall block the personal data if requested by the data subject or if, based on the available information, it is assumed that deletion would harm the legitimate interests of the data subject. Personal data blocked in this way may only be processed for as long as the purpose of processing which excluded deletion remains in effect.
17.2.9.9 The controller shall mark the personal data it processes if the data subject contests its accuracy or correctness but the inaccuracy or incorrectness cannot be clearly established.
17.2.9.10 The controller shall notify the data subject, and all parties to whom the data were previously transmitted for processing purposes, of any rectification, blocking, marking, or deletion. Notification may be omitted if it does not prejudice the legitimate interests of the data subject in view of the purpose of the processing.
17.2.9.11 If the controller does not comply with the data subject's request for rectification, blocking, or deletion, it shall inform the data subject in writing or, with their consent, electronically, within 25 days of receipt of the request, of the factual and legal grounds for the refusal. In the event of refusal, the controller shall inform the data subject of the possibility of judicial remedy and of recourse to the Authority.

17.2.10. Supervision

17.2.10.1 The heads of the organisational units carrying out processing shall be required to continuously monitor

compliance with data protection requirements, in particular the legislation referred to in the preamble and the provisions of this Policy.
17.2.10.2 The system administrator shall assist the work of the controller's organisational units and shall receive continuous information from them for maintaining the statutory records.
17.2.10.3 The Rector shall ensure compliance with the lawful order of processing by drafting internal regulations and submitting them to the Senate. The Rector shall authorise data linkages and data transfers.

17.2.11. Data Protection Officer

17.2.11.1 To ensure compliance with legal requirements for the processing of personal data and to support the exercise of data subjects' rights, the College shall appoint a Data Protection Officer, whose status is defined in GDPR Article 38 and in WP 243 Guidelines [GDPR Articles 37–38; Infotv. Section 25/L].
17.2.11.2 The Data Protection Officer shall facilitate the College's compliance with its obligations under the legal requirements governing the processing of personal data applicable to controllers and processors, in particular by:
a) providing up-to-date information on the legal requirements governing the processing of personal data and advising the controller, processor, and persons employed by them in carrying out processing operations on how to implement those requirements,
b) continuously monitoring and verifying compliance with the legal requirements governing the processing of personal data, in particular with legislation and with internal data protection and IT security policies, including clear task definition related to processing operations, enhancing the knowledge and awareness of employees involved in processing, and ensuring the regular implementation of audits,
c) facilitating the exercise of the rights of data subjects, in particular by investigating complaints lodged by data subjects and initiating the measures necessary at the controller or processor to remedy complaints,
d) providing professional advice and monitoring the conduct of data protection impact assessments,
e) cooperating with the bodies and persons authorised to conduct proceedings concerning the lawfulness of processing, in particular maintaining contact with the Authority to support prior consultation and procedures conducted by the Authority,
f) contributing to the development of the internal data protection and IT security policy [GDPR Article 39; Infotv. Section 25/M(1)].
17.2.11.3 During the term of their engagement and after its termination, the Data Protection Officer shall keep confidential any personal data, classified data, and any data qualifying as a secret protected by law or by a professional duty of confidentiality, as well as any other data, facts or circumstances that the controller or processor employing them is not required by law to make accessible to the public. [GDPR Article 38(5); Infotv. Section 25/M(2)]

17.3. Specific processing operations

17.3.1 Unified electronic student information and records system (Neptun)

17.3.1.1 The student register is the College's data processing that serves to document facts relating to student status; the scope of data recorded is defined in Annex 3, point I/B.1 of the NHEA.
17.3.1.2 Primary data collection takes place when the student status is established (enrolment). The responsible administrator at the Academic Affairs Office ensures the security of the data.
17.3.1.3 In accordance with the applicable legislation, the College records students' personal and sensitive data relating to student status, the determination and fulfilment of benefits, allowances and obligations, and to study and examination matters [NHEA Annex 3, title I/B; NHEA Decree §60], as well as the data of instructors, researchers and teachers to be reported to the Higher Education Information System (FIR) [NHEA Annex 3, title I/A], in the appropriate IT application, the Neptun Student Information and Records System (hereinafter: Neptun). It ensures students' continuous access to their personal and academic data recorded therein and is responsible for the security of the recorded data [NHEA Decree §34(1)–(2)]. Rules concerning Neptun—particularly its operation, data protection, system access, entry of records, data backup and the related procedures—are laid down in this Policy, the Study and Examination Regulations (SER), the IT and Security Policy (ITSZ), and the Neptun Operation and Management Policy.
Rules concerning Neptun—particularly its operation, data protection, system access, entry of records, data backup and the related procedures—are laid down in this Policy, the Study and Examination Regulations (SER), the IT and Security Policy (ITSZ), and the Neptun Operation and Management Policy.

17.3.1.4 Personal data from the student register may be transmitted—other than to the data subject—only to the recipients specified, and under the conditions set out, in point 4 a)–f) of title I/B of Annex 3 to the NHEA.
17.3.1.5 The academic administrator acting as data owner is responsible for uploading to the Neptun system, for the continuous maintenance of, and for ensuring conformity with personal identification documents and official records in respect of: student data, data stored on issued diplomas and certificates, and data stored on certificates issued to attest the successful completion of the final examination.
17.3.1.6 Instructors, as data owners, are obliged to enter into Neptun grades, examination dates, in-term assignments and other data related to academic requirements. The Academic Affairs Office provides reasonable support to instructors in this respect.
17.3.1.7 The designated data steward is responsible for uploading and continuously maintaining the data stored on employees in the Neptun teaching interface, as well as ensuring compliance with personal documents and certificates.
17.3.1.8 The designated data steward is responsible for recording, uploading and continuously maintaining institutional and programme data.
17.3.1.9 Data in the student registry may be processed for eighty years from the notification of the termination of the student status.
17.3.1.10 The rules concerning the student registry shall also apply to the personal data provided by applicants on the dedicated electronic interface of the College's website, with the provision that such data – as regulated in the Admission and Transfer Regulations [ATR 6.5] – may be processed exclusively in the context of the admission procedure, until the applicant acquires the right to student status. The range of personal data voluntarily provided by the applicant in this framework, and the purpose of processing, are identical to the scope of data and data processing purpose defined by law in the higher education admission system (Annex 3 I/B. of Njtv.), and – after successful admission, as a condition thereof – may be processed and linked as the primary data collection (enrolment) base data provision defined in point 17.3.1.2.

17.3.2. Employee Registry

17.3.2.1 The employee registry constitutes the College's data processing for documenting facts concerning higher education employment. The scope of data recorded is defined in Annex 3 I/A 1. of the NHEA. Data collection is carried out by the head of the Rector's Office – as the College unit responsible for human resources (preparatory and administrative) tasks – who also ensures data security. Uploading data into Neptun is the responsibility of the Director of Academic Affairs.
17.3.2.2 The College may process personal and special categories of data only in relation to employment, the establishment and fulfilment of benefits, allowances, obligations, for reasons of national security, and for the purpose of maintaining legally prescribed records, to the extent necessary and strictly for the stated purpose.
17.3.2.3 Duration of processing: – with the exception of payroll records that cannot be disposed of for pension insurance reasons – five years from the termination of employment.
17.3.2.4 The obligations relating to employee data provision and the further rules of personnel records are set out in the Employment Requirements System (ERS) [ERS 8.4.3].

17.3.3. Payroll and Employment Records

17.3.3.1 Payroll and employment records constitute the College's data processing for documenting facts relating to employment and other work-related legal relationships. The scope of data recorded, the purpose and duration of processing – subject to deviations recorded in the NHEA – are determined by Act I of 2012 on the Labour Code, as well as the applicable tax and social security legislation. Records not disposable for pension insurance reasons include: supporting payroll documentation (employment contracts, amendments to contracts, mutual agreements on termination of employment, employer's notices, employer's or employee's terminations, and other declarations, certificates, attendance sheets, as well as employment litigation records) and, based on such documents, TB (Social Security) and NAV (National Tax Authority) declarations, registration and deregistration forms, payroll slips and summaries.
17.3.3.2 Data in payroll and employment records may be used for establishing facts relating to the employee's employment or other work-related legal relationship, verifying classification requirements, payroll processing, tax and social security administration, and statistical data provision.
17.3.3.3 All management and supervisory rights relating to payroll and employment records fall within the competence of the Financial Director, who ensures compliance with data protection rules for both internal data processors and external data processors, including the conclusion and maintenance of data processing agreements.

17.3.4. Higher Education Information System

17.3.4.1 The institutional database, employee personal database, admission subsystem, and student personal database of the Higher Education Information System (FIR) contain the personal data specified in Annex 3 of the Onytv. and Annex 3 of the NHEA, as well as the additional data specified in Annex 6 of the NHEA Decree. The sectoral leadership information application of FIR (hereinafter: AVIR) and the Graduate Career Tracking System application of FIR (hereinafter: GCTS) contain data not classified as personal data by the minister.
17.3.4.2 The FIR records are operated by the Education Authority in accordance with the relevant legislation. On behalf of the College, with regard to FIR and its higher education admission subsystem (the felvi.hu portal), liaison with the Education Authority is carried out by staff members of the Academic Affairs Office appointed by the Rector at the initiative of the Director of Academic Affairs.
17.3.4.4 In the case of the GCTS, mandatory institutional data provision is based on voluntary online questionnaires, conducted using a uniform methodology and questionnaire, among current students and those who obtained an absolutorium one, three, and five years previously. definition, deadline, frequency, method of data provision, as well as the methodological description and questionnaire related to the data provision are published on the website of the ministry exercising sectoral management. The results of graduate career tracking studies must be published at least annually on the College website as part of the annual quality assurance report.
17.3.4.5 From the higher education information system – in the absence of a legal provision to the contrary – personal data may only be disclosed at the request of, or with the written consent of, the data subject, with simultaneous notification of the data subject. The minister is responsible for the lawfulness of data processing within the higher education information system. Data subjects are entitled to access their own data in the higher education information system. Data subjects are entitled to access their own data in the higher education information system. The data subject is entitled to request the correction or deletion of their data stored in the higher education information system – except for legally mandated processing – from the higher education institution providing the data, i.e., the College. Access, correction, and deletion of data by the higher education institution are free of charge in all cases.
17.3.4.6 The designated data steward is responsible for managing and saving system messages sent by the FIR. The system administrator supervises and, as necessary, assists the activities of those responsible.

17.3.5 Student ID Card

17.3.5.1 Upon the student's application submitted in the NEPTUN system, the College initiates the issuance of a student ID card with the Education Authority through the Higher Education Information System (FIR), in the Institutional System of Educational Certificates (OKTIG), and performs the institutional tasks defined in Government Decree 362/2011 (XII. 30.) on educational certificates in connection with this process.
17.3.5.2 The rules of the College regarding the handling of student ID cards, validation stickers, and other forms, as well as institutional records, are contained in a rector's directive, which defines specific data management tasks and designates the administrators responsible for them.

17.3.6 Hungarian State Scholarship Register

The Education Authority records the academic lifecycle, training data, and personal and address data of students receiving Hungarian state (partial) scholarships during their studies, based on the data stored in the FIR. Institutional liaison regarding compliance with the conditions of the Hungarian state scholarship is carried out by staff members of the Academic Affairs Office appointed by the Rector at the initiative of the Director of Academic Affairs.

17.3.7 Student Loan (Diákhitel)

17.3.7.1 The College – in cooperation with the Student Loan Centre Ltd. (hereinafter: Student Loan organisation), in the manner defined by Government Decree 1/2012 (I. 20.) on the student loan system – establishes the procedure for the verification of student status. Based on this, the College certifies the existence and changes of student status and, upon request by the Student Loan organisation, reconciles on a monthly basis, electronically, the data prescribed by law concerning the lawful disbursement of student loans with the Student Loan organisation, by comparing and verifying the data provided by the organisation with the data stored in Neptun, and informing the organisation of the results:
a) the student's personal data,
b) the fact of the student's enrolment for a training period in order to pursue studies,

c) the fact of the existence, suspension, or termination of student status,
d) the type of funding of the programme pursued by the student,
e) the amount of self-financed or tuition fees payable by the student,
f) the student's tax identification number,
g) the closing date of the student's absolutorium [Government Decree, Section 13 (4)].
17.3.7.2 The organisational unit of the College responsible for student loans is the Academic Affairs Office. The College's student loan liaison officer is appointed by the Rector in agreement with the Director of Academic Affairs. In addition to the data reconciliation and issuance of student status certificates referred to in point 17.3.7.1, the student loan liaison officer ensures that the notices sent by the Student Loan organisation for publication are communicated to students, and also performs other tasks specified in the cooperation agreement concluded with the Student Loan organisation.
17.3.7.3 Within the framework of cooperation with the Student Loan organisation, the College performs data processing tasks under contract, subject to the provisions of the agreement concluded with the Student Loan organisation. The rector's directive – issued in agreement with the Financial Director and the President of the Student Government – contains the Procedural Rules for verifying, receiving, and forwarding the standard form used for the assignment of general-purpose student loans.

17.3.8 Bursa Hungarica

17.3.8.1 The list of personal and special categories of data processed, and the rules of processing within the framework of the Bursa Hungarica Municipal Higher Education Scholarship operated in cooperation between the Government and local municipalities, are set out in Annex 4 of the NHEA.
17.3.8.2 The Financial Director, through the Academic Affairs Office – for the purpose of disbursement as specified in Chapter 3.2.2.1.5 of the Student Tuition and Benefits Regulations, in NEPTUN – processes the data.
17.3.8.3 The Director of Academic Affairs forwards data on the status of student enrolment to the grant management organisation (Human Resources Support Manager), as well as to the local municipality providing the support via the electronic platform operated by the grant management organisation.

17.3.9 Statistical Data Provision

17.3.9.1 The College fulfils central and sectoral statistical data provision obligations to the Hungarian Central Statistical Office (KSH) through accountants as data processors. Management and supervisory rights concerning them fall within the competence of the Financial Director, who ensures compliance with data protection rules, including the conclusion and maintenance of the data processing agreement.
17.3.9.2 The task of providing accountants with supplementary data that cannot be compiled from accounting records, through the Financial Director, lies with the designated data steward, who is also obliged to ensure that statistical data provision is always consistent with other external data provisions (particularly data supplied to the Education Authority and the supervising ministry).

17.3.10 Data Processing for Quality Assurance and Quality Enhancement

The College's data processing for quality assurance and quality enhancement is regulated within the limits set by law by the College's Quality Assurance and Quality Enhancement Regulations [QAQER 10.2.12–18, 10.4 and 10.5].

17.3.11 CCTV System

For crime prevention and asset protection purposes, a closed-circuit CCTV system operates on the College premises. Its detailed rules are set out in Annex 4 (CCTV System Regulations). The legal basis for processing: the controller's legitimate interest (OOR 17.2.1.1 F).

17.3.12 Access Control System

On the College premises – for crime prevention and asset protection purposes – an access control system is operated jointly with the property owner, the Dharma Gate Buddhist Church as Maintainer. This ensures electronic access to administrative and semi-administrative rooms, as well as access to buildings outside teaching hours. The data of the access control system are processed in a closed IT system. The legal basis for processing: the controller's legitimate interest (OOR 17.2.1.1 F). The issuing and withdrawal of access badges, as well as the operation of the access control

system, fall within the competence of the caretaking service jointly managed by the Rector and the Church Directorate, for which the system administrator or their substitute provides IT support.

17.3.13 Websites

17.3.13.1 The operation and maintenance of the College's websites fall within the competence of the Director of Academic Affairs, including the related content provision [OOR 2.5.4.10.5]. The system administrator or their substitute provides IT support for this, while the data stewards provide up-to-date information.
17.3.13.2 The College websites must have a uniform structure and layout. To prepare, adopt, monitor, and further develop professional decisions regarding a unified image, the Rector establishes an ad hoc committee (Marketing Group). The Director of Academic Affairs, the system administrator, a delegate of the Quality Management Committee, and a representative of the Maintainer – together with other persons invited by the Rector – participate in the committee's work with voting rights. The rector's directive, issued in agreement with the Director of Academic Affairs, contains the formal and substantive criteria developed by the committee for compliance with institutional standard ESG 1.8, as well as the regular procedural rules for their implementation. The rules for publishing public-interest information on the website are set out in Chapter 17.4.
17.3.13.3 The processing of website visitors' personal data may only take place to the extent necessary for the use of website services, in accordance with their provisions, and in full compliance with applicable EU and Hungarian legal requirements. The websites must provide visitors with a concise, easily accessible, and understandable privacy notice, which, in clear and comprehensible language, and if necessary with visual aids, contains the information regarding the processing of their personal data as defined by the GDPR and the Information Act.

17.3.14 Electronic Mail and Mailing Lists

17.3.14.1 The issuing and withdrawal of e-mail addresses belonging to the College domain (tkbf.hu; dgbc.hu), and the operation and supervision of the related interfaces, are the responsibility of the institutional officer designated by the Rector. The Rector may regulate, by directive, the operation of the e-mail system, the rules for issuing and withdrawing e-mail addresses, as well as the rules for using e-mail addresses, taking into account the provisions of this Regulation, the IT Security Regulations (IBSZ), and other College regulations.
17.3.14.2 The Rector of the College – in agreement with the Maintainer Church – is entitled to decide on the establishment or termination of College mailing lists (currently: E-Senate, Hivatalos, Tanárok and Diákinfo).
17.3.14.3 The College, jointly with the Maintainer Church, operates an alumni system for the purpose of graduate career tracking, the mailing list of which is the Church mailing list of Buddhist teachers, to which students are added after successfully completing their final examination.
17.3.14.4 For the mailing lists operating at the College, the person or body designated as list moderator – taking into account this Regulation, the IT Security Regulations (IBSZ), and the College's other regulations – is authorised to define the "list usage, data-management and ethics policy" applicable to the specific list, in the form of a Church Directorate instruction (Buddhista tanítók, Egyház hírek, Egyháztanács, Párbeszéd, Támogatók), a rector's instruction (E-szenátus, Hivatalos, Tanárok), or – in the case of Diákinfó – rules adopted by the Student Representation.
17.3.14.5 A concise, easily accessible and easily understandable privacy notice concerning electronic mail and mailing lists must be placed for data subjects on the official website. It must, in clear and comprehensible language – and, where necessary, with visual presentation – contain the information on the processing of their personal data as defined by the GDPR and the Information Act. Data subjects must also be informed by e-mail about how to access and about updates to the privacy notice, ensuring the possibility to unsubscribe.

17.3.15 Data Processing for Grant Applications

17.3.15.1 Data processing for grant applications is carried out with the content, purpose, method and duration defined in the sectoral data-processing rules applicable to the given call.
17.3.15.2 Data processing related to international mobility (Erasmus+, Campus Mundi) is performed by the International Office; disbursement is executed through the Financial Director.
17.3.15.3 Data processing related to support from European Union funds is the task of the College data controller designated for this purpose by the Rector as project owner, who also performs the data-processing tasks owed to the grant-managing body for the given project. To the extent and for the purpose necessary to perform their tasks, the processed data may be forwarded to the project manager, the project financial director, the professional lead, the

Financial Director, and the person exercising supervisory oversight on behalf of the Maintainer.

17.4 Publication of Public-Interest Data; Handling of Data Requests

17.4.1 Pursuant to Section 33 (1) of the Information Act, the College shall make the public-interest data that must be published available on its official website (www.tkbf.hu) in digital form (indicating date and validity) to anyone, without identification, without restriction, printable and copyable in full and in parts without data loss or distortion, and free of charge for viewing, downloading, printing, copying and network transfer (hereinafter: electronic publication). Access to the published data shall not be conditional upon the provision of personal data.
17.4.2 Unless the Information Act or other legislation provides otherwise, electronically published data may not be removed from the website. In the event the College ceases to exist, the obligation of publication shall pass to its legal successor.
17.4.3 In a structure relevant to its activities, the College shall publish the data defined in the general publication list set out in Annex 1 to the Information Act. Legislation may define further data to be published for certain sectors or types of bodies performing public duties (hereinafter: special publication list). The Rector – after seeking the opinion of the Authority – and legislation, with effect covering bodies performing public duties under their direction or supervision or part thereof, may define additional categories of data that must be published (hereinafter: individual publication list).
17.4.4 Tasks related to publication, correction, updating and removal shall be performed by the data steward together with the Director of Academic Affairs responsible for the website and the competent managers.
17.4.5 In fulfilling requests to access public-interest and data public on grounds of public interest, the College shall proceed in accordance with Sections 28–31 of the Information Act.
17.4.6 The assessment and fulfilment of requests to access public-interest data fall within the powers and duties of the Rector, or, in the event of impediment, the Vice-Rector.
17.4.7 In the event of refusal of a request to access public-interest data, the College shall inform the data subject of the possibility of judicial review and of applying to the Authority. The College shall keep records of refused requests and the reasons for refusal, and shall inform the Authority of the contents thereof by 31 January of the year following the reference year [Information Act Section 30 (3)].

17.5. Miscellaneous and Final Provisions

17.5.1 The Rector is authorised to designate data stewards by rector's instruction.
17.5.2 In the exercise of administrative-organisation powers – on information-security, data-protection and cost-efficiency grounds – the Rector is entitled to engage an external service provider to perform part of the tasks of the IT Group [OOR 2.5.4.14], or to share those tasks between the external service provider and the academic IT specialist employed within the Academic Affairs Office [OOR 2.5.4.8].
17.5.3 The primary aim of this policy is to support its users; therefore, it must be made readily accessible—alongside the data management regulations found in other volumes of the College's Regulations (HKR, FKR, EKR)—both electronically through a dedicated online platform and in printed form at the Rector's Office.
17.5.4 This Regulation enters into force on 19 May 2017, based on Senate Resolution No. 30/2017. (05.18.) of 18 May 2017, and forms Annex 9 to The Dharma Gate Buddhist College Regulations, Vol. IV: System of Other Regulations (EKR). At the same time, the cover page of The Dharma Gate Buddhist College Regulations is supplemented in Vol. IV: System of Other Regulations (EKR) with the designation: "Annex 9: Data Protection and Data Management Policy".
17.5.5 The consolidated version of this Regulation with amendments (AASZ 2019) enters into force on 26 September 2019, based on Senate Resolution No. 43/2019. (09.26.) of 26 September 2019.

Issued in Budapest, on 26 September 2019.

Gábor Karsai rector