INTERNATIONAL BUSINESS SCHOOL
GENERAL DATA PROTECTION REGULATION

(IBS GDPR)

This regulation was approved by resolution No. 3/2018 of the Senate
on 9 May 2018

The Senate of IBS International Business School

- With reference to Section 18 of Act No. 204 (2011) on National Higher Education (hereinafter: HE Act),

- With reference to Government Decree No. 87/2015 on the implementation of certain provisions of Act No. 204 (2011) on National Higher Education (hereinafter: Government Decree on HE Act)

- With reference to Section 24 Article (2) point d) of Act No. 112 (2011) on Informational Self-determination and Freedom of Information (hereinafter: Information Act)

- With reference to 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) (hereinafter GDPR Regulation),

defines the institutional framework for data processing and transfers at the School in the present regulation (hereinafter IBS GDPR):

The purpose and scope of the present regulation (IBS GDPR)

Section 1

(1) IBS GDPR aims to define the rules that apply in processing and transferring data recorded at IBS International Business School (hereinafter: the School) and to ensure the fundamental rights of data protection and the legal requirements of data security; to prevent the unlawful alteration and unauthorised disclosure of, or access to, data; and to provide an institution-wide policy for the disclosure of data of general interest.

(2) IBS GDPR applies to

(a) all employees of the School as well as all persons in an employment relationship with the School,

(b) all students of the School, irrespective of the mode of delivery,

(c) all data controlled by the School, and

(d) all organizational units that perform data processing.

Data protection terminology

Section 2

(1) Personal data:

Any information relating to an identified or identifiable natural person, especially the name, the or one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person; as well as any conclusions drawn about that natural person based on the data.

(2) Special categories of personal data:

(a) Personal data revealing racial or ethnic origin, nationality, political opinions or party affiliation, religious or philosophical beliefs, or trade union membership, and data concerning a natural person's sex life or sexual orientation.

(b) data concerning health or habits as well as personal data relating to criminal convictions and offences.

(3) Data relating to criminal convictions and offences:

Personal data originating in the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which may be attributed to the data subject as well as personal data related to any criminal record.

(4) Data of public interest:

Data processed by the School as well as information or knowledge related to its activities or those originating in connection with its public-service mission, excluding personal data, irrespective of its method of processing or whether individual or collated in nature. As such, the term covers data related to authorisations; responsibilities; organisational structure; professional activities (including the evaluation of their effectiveness); regulations pertaining to the data types controlled and to those controlling the School’s operations; as well as financial and contractual data.

(5) Data processing:

Any operation or set of operations which is performed on data or on sets of data, such as collection; recording; organisation; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure; alignment or linking; restriction; erasure or destruction as well as preventing the subsequent use of data; creating photo, sound, or video recordings; or recording physical features (e.g., finger or palm prints, DNA, retina scan) that are capable of identifying the subject.

(6) Data Controller:

The School, its organizational unit or an employee that determines the purposes and means of the processing of personal data, takes and executes decisions regarding data processing (including the method used) or mandates another data processor to do so.

(7) Technical processing:

Performing technical tasks related to data processing, irrespective of the method and device used to perform the operations and the location, provided that the technical task is performed on the data.

(8) Data Processor:

A natural or legal person or an organization that is not a legal person which processes personal data on behalf of the controller under contract (including those mandated by laws and regulations) with the data controller.

(9) School Data Protection Officer:

A person with appropriate qualifications who contributes to, provides assistance with, and prepares decisions that concern data processing; oversees and monitors compliance with the applicable laws, the present regulation (IBS GDPR), and the measures to ensure data security; investigates data processing reports; maintains the record of processing activities; provides awareness-raising and training in relation to the protection of personal data; and undertakes the other responsibilities specified in the present regulation or other data protection provisions. At the school, as mandated by the Rector, the Secretary General undertakes the role of Data Protection Officer.

(10) Data protection:

Any rule, procedure, tool, or method or set of rules, procedures, tools, or methods that ensure the limitation of processing as well as the legal protection and the informational self-determination of data subjects.

(11) Data transfer:

Making the data available to a specified third party.

(12) Disclosure:

Making the data available to anyone.

(13) Data erasure:

Making the data unrecognizable in such a way that their recovery is no longer possible.

(14) Data destruction:

Complete physical destruction of the media that contains the data.

(15) Marking data:

Adding identification to the data in order to distinguish it from other data.

(16) Restriction of processing:

Marking of stored personal data with the aim of limiting their processing in the future definitely or indefinitely.

(17) Set of personal data:

Any set of personal data processed within a filing system.

(18) Third country:

Any country that is not a member of the European Economic Area.

(19) Data Subject:

A natural person who is identified or, directly or indirectly, identifiable on the basis of personal data.

(20) 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.

(21) Objection:

A statement by the Data Subject objecting the processing of their personal data and requesting the termination of processing or the erasure of the data.

(22) Employee:

Any person employed by or in an employment relationship with the School (including student employment contracts).

(23) Data manager:

The public-service body that has generated the data to be published electronically or during whose operation the data have been generated.

(24) Third party:

A natural or legal person, public authority, agency or body other than the data subject, data controller, data processor.

(25) EEA state:

A member state of the European Union and any other state party to the agreement on the European Economic Area, as well as a state the citizens of which enjoy equal legal standing with nationals of the states of the European Economic Area on the basis of an international treaty between the European Union and its member states and the given state.

(26) Binding corporate rules:

Personal data protection policies which are adhered to by a controller or a group of controllers established on the territory of minimum one EEA state and approved by the National Data Protection and Information Authority (hereinafter referred to as "the Authority"), ensuring the protection of personal data through the unilateral commitment of the data controller or a group of data controllers for transfers or a set of transfers of personal data to a controller or processor in one or more third countries.

(27) Personal data breach:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed.

Protection of personal data

Data Processing

Section 3

(1) Personal data, including special categories of personal data, which are required to be registered and to be processed by the School and covered by this regulation (IBS GDPR), as well as the data processing and the transfer of data are governed by Appendix 3 of the HE Act. These data may be used for statistical purposes and may be transferred for statistical purposes in a manner which do not permit or no longer permit the identification of data subjects.

(2) In case of recording personal data, including special categories of personal data, not included in Appendix 3 of the HE Act, the Data Subject must be informed about the purpose of, the legal basis for, the identity of the data controller, the duration of the data processing and the identity of those who may access the data. The data subject should also be informed whether he or she is obliged to provide the personal data. In case the data subject is obliged to provide the personal data, then the regulations that provide the legal basis for the obligatory data provision must also be identified. The information shall also include the rights and appeals available to the data subject related to data processing.

(3) Similarly, the School may conduct its employability survey only based on voluntary data provision. In the case of voluntary reporting, the data subject shall be informed that he or she is not obliged to provide the personal data.

(4) Unless a longer archival period is stipulated by the applicable laws and regulations, including the archiving regulations of the School, employees' personal data may be processed for up to five years from the date of the termination of their employment. Students' personal data may be processed up to eighty years from the termination of their student status.

(5) The personal data of employees and students, with the exception of the employee's name and position, may solely be processed for purposes related to and to the extent necessary for employment, benefits, allowances, the exercise of citizens' rights and responsibilities, national security, the processing of records as stipulated by the HE Act.

(6) The School may, with the exceptions provided for in Articles 7 and 8, communicate facts, data and opinions concerning employees to third parties only in the cases specified by law or with the consent of the employee. For special categories of personal data, written consent must be solicited.

(7) In a process initiated by the data subject, their consent to processing the relevant data needs to be presumed.

(8) If, the data subject is physically or due to other unavoidable reasons incapable of giving consent, in order to protect the essential interests of their own person or to the aversion or prevention of perils threatening their or others' life, health or possessions, the personal data of the data subject can be processed to the necessary extent while the above barriers are present.

Combining data

Section 4

(1) Data defined in Appendix 3 of the HE Act managed by different organizational units of the School may be combined if necessary. These may be combined with data from other data controllers only if justified and only subject to the data subject's consent or if permitted by law, provided that the conditions for data processing may be satisfied for each personal data.

(2) The data controller(s) that initiate(s) the combining of data shall notify the School Data Protection Officer by completing the form in Annex 2 so that the relevant facts may be registered by the School.

(3) In order to protect the files that are processed by electronic means in different filing systems, appropriate technical solutions must ensure that the data stored in the filing systems cannot be directly combined and attributed to the data subject, unless permitted by law.

Disclosure of personal data

Section 5

(1) The disclosure of personal data processed at the School is prohibited, unless prescribed by law.

(2) Students' grades, examination results and whether or not they receive social support constitute personal data. In case of disclosure, instead of the names codes shall be used.

Technical processing

Section 6

(1) The rights and responsibilities of technical processors with regard to the processing of personal data shall be defined in the relevant contract.

(2) The technical processor shall be responsible for the processing, alteration, erasure, transfer and disclosure of the personal data within the scope of its activity or within the limits set by the data controller.

Data transfer

Section 7

(1) Data defined in Appendix 3 of the HE Act managed by the different organizational units of the School may be transferred to other organizational units within the School in order to perform administrative and organizational tasks related to employment or student status, to the extent and for the duration necessary for the performance of the task.

(2) Data defined in Appendix 3 of the HE Act may be transferred to external bodies as specified therein.

(3) In cases not covered by Article 1, the intent to transfer data within the School shall be made to the School Data Protection Officer on the form in Annex 3 to this Regulation. Data transfer may be effected following the written consent of the School Data Protection Officer. In case of regularly occurring data transfer, the consent is valid until withdrawal. Facts pertaining to the data transfer are recorded by the School Data Protection Officer.

(4) Request for data transfer from a body or a private person outside the School may only be fulfilled if the conditions specified in Article 5 are met, except for the mandatory data transfers specified in Section 19 Article 3 of the HE Act.

(5) Data managed by the School – except those defined in Appendix 3 of the HE Act – may only be transferred if the Data Subject has given written consent or is explicitly required by law and if the School has ascertained that the conditions for processing personal data are met. The data subject may also give an

advance authorization, for a specific period, for a specific set of bodies that may request data, and for the scope of the data that may be subject to transfer.

(6) The data controller or data processor shall, either directly or through its superior, inform the School Data Protection Officer about data transfers to bodies specified in Appendix 3 to the HE Act on a quarterly basis.

(7) In line with Section 42 of Act 125 (1995) on national security services, all data relating to inquiries from national security services constitute state secret, of which no other body or other person shall be informed.

(8) Any data transfer upon an external request - except for the requests specified in Article 6 - may only be effected following the written consent of the School Data Protection Officer after the due submission of the application form in Annex 3 of the present Regulation. The fact of data transfer – with the exception of the cases referred to in Article 6 – must be reported to the School Data Protection Officer, who shall register it.

Data transfer abroad

Section 8

(1) Transfer of data to an EEA Member State shall be considered equal to transfer of data within the territory of Hungary. The language of data transfers by the School abroad shall be Hungarian and/or English.

(2) Personal data (including special categories of personal data) may be transferred to a third country only if the data subject expressly consented to it, if it is permitted by law, or if the conditions set out in the Information Act or the GDPR Regulation are met, and there exists an adequate level of protection by the third country when processing the personal data transferred.

(3) Personal data may be transferred to a third country for the purposes of the international treaty on the international legal aid and the avoidance of double taxation, for the purpose, conditions, and scope of data specified in the treaty.

(4) In the case of data processing where data transfer abroad is expected, the data subjects must be made aware of this before data collection.

(5) The facts relating to the provision of data abroad shall be documented in accordance with Section 7 (8).

Data security

Section 9

(1) The data processor shall ensure the security and quality (accuracy, consistency, completeness, timeliness) of the data.

(2) The data controller and the data processor, within its sphere of activities, shall provide for data security, in particular, protection against unauthorized access, alteration, transfer, disclosure, erasure, destruction, damage and loss, as well as the protection against unavailability of data caused by a change in the technology used. All data processors are required to develop and maintain the technical and organizational measures and procedural rules necessary to enforce data protection in order to ensure the security of personal data managed and processed both automatically and manually.

(3) Employees responsible for data processing or technical processing are required to treat and retain the personal data they have access to as professional secret.

Records of processing activities

Section 10

(1) All non-statutory data processing of the School shall be recorded. Recording is initiated by the data controller with the School Data Protection Officer on the form in Annex 1 prior to data processing.

(2) The Data Controller shall keep a record of the transfer of the data in order to control the lawfulness of the transfer and to provide information for the data subject. The records shall contain the date, the legal basis for, and recipient of the data transfer, the definition of the scope of the data transferred and any other statutory data. If the law or the rules on records management in the School do not provide for a longer period of time this register shall be retained for a period of five years for personal data and a period of 20 years for special categories of personal data.

Rights of the Data Subject and their enforcement

Section 11

(1) The data subject may request information about the processing of their personal data, in Hungarian or in English, and may request that their personal data be rectified or, with the exception of statutory data processing, erased or restricted.

(2) At the request of the data subject, the information shall be provided by the data controller in Hungarian or English, and it must include the data of the data subject processed by the School; their sources; their purposes and legal basis; the duration of data processing; the data processor's name, address and its activities that concern data processing; the circumstances of the personal data breach, its effects, and the measures taken to remedy it; and, if personal data of the data subject has been transferred, the legal basis and the recipient of the transfer.

(3) At the request of the data subject, the data controller shall, in the shortest possible time, but no later than 25 days after the submission of the request provide information on the data it has processed, the purpose of, the legal basis

for, and the duration of the data processing and the transfer of the data in writing and in an understandable form.

(4) The information in Article (3) shall be provided free of charge if the applicant for information has not yet submitted an information request for the same area in the current year. In other cases, a cost reimbursement can be established, the amount of which is determined by the data controller processing the requested data, taking into consideration the amount of data requested and the time spent on providing the information. The reimbursement will have to be refunded if the processing of the data was illegal or the request for information has led to rectification.

(5) Provision of the information may only be denied in the cases defined by the Information Act Section 9 (1) (data received from abroad) and Section 19 (external and internal security of the state, and protection of the rights of the data subject or others).

In such cases, the data controller shall inform the data subject in writing of the legal grounds for refusal and inform them about possibility to seek remedy in court and to appeal to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter: the Authority). The School Data Protection Officer shall be informed of the refusal of the information, who shall notify the Authority of the applications rejected in a given year by 31 January of the following year.

(6) If the personal data is not consistent with the reality and the data corresponding to the reality is available to the data processor, the data processor must correct the data.

(7) Personal data shall be erased if its processing is unlawful if – with the exception of mandatory data processing – the erasure is requested by the data subject, if it is incomplete or incorrect and this status cannot be legally remedied and if the erasure is not prohibited by law. The data must also be erased if the court or the Authority has ordered it or the purpose of the data processing has ceased to exist or the deadline for storing the data specified in Section 3 (3) has expired.

(8) Personal data shall be restricted instead of erased if the Data Subject requests so or if, based on the information available, it may be assumed that the erasure would prejudice the legitimate interests of the data subject. Personal data thus restricted may only be processed as long as there exists a data processing purpose that prevents the erasure of the personal data.

(9) The data controller shall mark the personal data it processes if the data subject disputes its correctness or accuracy but the incorrect or imprecise nature of the disputed personal data cannot be clearly identified.

(10) The data subject as well as and all those that have previously received the data for the purposes of processing shall be notified about the correction, the restriction, and the erasure of the data. The notification may be omitted if it does not prejudice the legitimate interest of the data subject with a view to the purpose of the data processing.

(11) If the data controller fails to comply with the correction, restriction or erasure request of the data subject, it must notify the applicant in writing of the factual and legal grounds for rejecting the application within 30 days of receipt of the request. The communication must include court remedies and the possibility of appeal to the Authority.

(12) If the data subject objects the data processing on grounds of Section 21 of the Information Act, the data controller shall investigate the case, make a decision, and inform the applicant in writing within the shortest possible time but within a maximum of 15 days from the submission of the request.

(13) If the objection is upheld, then data processing, including further data collection and transfer, shall be discontinued, the data shall be restricted, and any person to whom the personal data affected by the objection had been previously transferred shall be notified of the decision.

(14) If the data subject disputes the decision of the data controller or if the data controller fails to comply with the deadline set out in article (12), the data subject may refer the decision to the court within 30 days from being informed of the decision or from the day of the deadline.

(15) The data controller shall maintain records in order to enable the School Data Protection Officer to control the measures related to personal data breaches and to keep the data subject informed. The records shall include the personal data concerned, the scope and number of data subjects concerned, the date, circumstances, effects of the personal data breach and the measures taken to remedy it, as well as the other data specified in the law regulating data processing.

Monitoring

Section 12

(1) Compliance with the provisions relating to data protection, and the present Regulation (IBS GDPR) in particular, has to be continuously monitored by the heads of organizational units responsible for data processing.

(2) The School Data Protection Officer advises the data controller organizations with their advice and opinion. They are authorized to access data processing. They can request information from the heads and staff of the data processing units orally or in writing.

(3) The School Data Protection Officer shall ensure that the legal order of data processing is maintained by reviewing the rules, minutes and records of data processing. In the event of a legal violation, the School Data Protection Officer must order the data controller to discontinue the violation.

Data processing areas

Student register

Section 13

(1) The student record is a data processing system to document students' legal status, the legal basis of which are the HE Act, Government Decree on HE Act, and the School's Organizational and Operational Rules and Regulations.

(2) For the purposes of student registration, the School operates an integrated central information system. Central administration tasks that are not supported by the study IT system may be solved with other IT systems.

(3) The student record data can be used for the management of the students' learning and examination duties, for awarding, disbursement and payment of scholarship or tuition fees and for all organizational and administrative tasks related to the students' legal status.

(4) The coordination of the study IT system at School level as well as the coordination of the work of units involved in the operation, development and maintenance of the system shall be provided by the Centre for Student Services.

Section 14

(1) The data of the student register shall be provided from the central and institutional enrolment database and from the study contract signed by the student. The data of the educational and administrative staff are uploaded to the system by the organizational units based on their own records. The data are entered into the database in writing (electronically or on paper). No data may be entered into the database based on oral communication.

(2) Method of data entry:

The data entered in the database cannot differ from the data in the data source document. The person entering the data is responsible for the consistency of the data.

If the data contained in the source document is incomprehensible, unreadable, controversial or incomplete, it cannot be entered into the database. In such a case, the correction or completion of the document serving as source must be requested from the data subject or, if the information does not originate from the data subject, from the issuer of the original document.

(3) Student information is managed by the Centre for Student Services and the persons tasked with this role at the relevant organizational units.

Section 15

(1) Records are maintained in a computer database. Data controller units may transfer data only with the permission of the responsible manager of the School, in compliance with the present regulation. The transfer of data beyond those in Section 7 (1) of this Regulation may be initiated by completing the form in Annex 4. When judging the validity of the data transfer, the issue whether the organizational unit requesting it is eligible to handle the requested data must be taken into account.

(2) Data on the study IT system shall be protected against unauthorized access, alteration, transfer, disclosure, erasure or destruction as well as accidental destruction and damage. Providing this protection is the responsibility of the system operator (the IT department of the School), the Centre for Student Services (CSS), and the persons and units responsible for data processing and technical processing.

(3) In order to ensure the security of the data stored on the servers, the IT unit operating the system shall take the following actions and maintain the security consistently at a high level in a way that:

(a) servers are stored in closed rooms with adequate physical protection. Environmental and technical conditions for the operation of the servers are provided for;

(b) security backups are made of the active data of the personal databases on a daily basis. The backup and the production database must be hosted on storage devices on different locations;

(c) servers containing personal data are not accessible via a direct network path and that the system cannot be hacked with network access;

(d) servers can be shut down properly without loss of data in the event of a power blackout;

(e) anti-virus protection is provided for the servers;

(f) in case access to the database server is through terminal servers, the allocation and withdrawal of credentials required for access to terminal servers is provided, granting the minimum permissions for the purposes of data processing;

(g) the system administrator password of the server and the IT system is kept locked in a fireproof metal cartridge. Passwords must be changed at least every 6 months.

(4) The system for the student register shall allow for the logging of data modifications, their dates and executor.

Tutor and researcher register

Section 16

(1) The register of tutors and researchers involves processing data for documenting the facts related to the employment of tutors, researchers and teachers, the legal basis for which is provided for by the HE Act, the Labour Code and their implementing regulations, the Civil Code and the School's Organizational and Operational Rules and Regulations.

(2) The data of the tutor and researcher register shall be used to establish facts related to the employment contracts (contract of employment or other contractual relationship) and for statistical data provisions.

(3) The processor of the tutor and researcher register is the Centre for Academic Services.

Section 17

(1) The tutor and researcher register shall contain the data of all persons employed full-time by the School and those employed in other legal forms pursuant to Section 16 (1).

(2) The data for the tutor and researcher register shall be provided by the data subjects. Primary data collection takes place when the employee (employment) relationship is established.

(3) The register shall be managed in a mixed system by computer and manually. Data security is provided for by the data controller.

(4) Within the School, only data requests from the Rector, the Finance and Logistics Centre, the Chief Administration Officer and the heads and HR administrators of the units where the data subject performs their duties shall be fulfilled from the tutor and researcher register.

Pay roll and labour register

Section 18

(1) The pay roll and labour register involves data processing for the documentation of the tutor and researcher and other employment relationships (employees), the legal basis of which is the HE Act, the Labour Code, their implementing regulations, the Civil Code and the School's Organizational and Operational Rules and Regulations.

(2) The records of the pay roll and labour register may be used to establish facts relating to the legal status of the employee, to justify the fulfilment of classification requirements, pay-roll accounting, social security administration and statistical reporting.

(3) The pay roll and labour register is managed by the Finance and Logistics Centre.

Section 19

(1) The pay roll and labour register contains data about all employees of the School.

(2) The register is managed on computer. Data security is provided by the data controller.

(3) Within the School, only data requests from the Rector, the Finance and Logistics Centre, the Chief Administration Officer and the heads and HR administrators of the units where the data subject performs their duties shall be fulfilled from the pay roll and labour register.

Disclosing data of public interest

Section 20

(1) The School shall publish all the data defined by Annex 1 of the Information Act on its website in digital format, available for anyone without identification, without limitation, in printable format that can be copied without loss of data or distortion, free of charge for access, download, printing, extraction and network data transfer.

(2) Data are updated at the intervals specified by the Information Act with the coordination of the School Data Protection Officer.

Accessing data of public interest

Section 21

(1) The School shall comply with the obligation to provide information regarding individual requests for data of public interest by publishing the present regulation on its website.

(2) Access to data of public interest may be requested by anyone in writing or electronically. Requests made orally shall be recorded in writing in the form of a memo, no later than two working days from the submission of the oral request. The date of receipt of the oral request is the date of filing the request in written form. The School shall also accept a request for public information submitted on its website by filling out a form.

(3) The personal data of the data requester may only be processed if it is necessary for performing and charging for the claim and only for the period specified in the Information Act.

(4) The School shall not be required to comply with the request for information if the claimant does not give their name, the identity of a non-natural person, and

the contact details to which any information and notice related to the data request may be provided.

(5) Requests for data of public interest received, irrespective of the channel of communication, shall be forwarded to the School Data Protection Officer. The person entitled to communicate with the requester of data of public interest is the School Data Protection Officer. If a request for data of public interest is received by any unit, the given organizational unit shall immediately forward it to the School Data Protection Officer.

(6) In addition to the duties set out above, the School Data Protection Officer shall be responsible for the following when providing data of public interest:

(a) coordinating the process of supply the data, enforcing the law,

(b) liaising with the organizational unit designated for providing the data,

(c) responding to the request,

(d) recording requests and refusals,

(e) fulfilling the necessary data disclosure,

(f) fulfilling all statutory duties as data protection officer.

(7) Depending on the subject of the request received, the School Data Protection Officer shall, without delay (within a maximum of 3 days), assign it to the unit responsible for the provision of the data and for compiling the response, and, with the designation, forward the request for data of public interest to the unit. Selection is made in accordance with the following principles:

(a) in the case of educational, research-related data requests, the unit responsible for compiling the response is the Centre for Academic Services;

(b) the organizational unit responsible for compiling the responses to data requests concerning the Student Union: SU;

(c) in the case of data requests on operations, the unit responsible for compiling the response: the Rector's Office.

(8) The Rector of the School decides on the fulfilment of the request, on the possible reimbursement of expenses and on its extent, taking into account the recommendation of the School Data Protection Officer and the organizational unit designated for the data supply.

(9) The organizational unit designated for the provision of data shall be obliged to comply with the data supply or refuse to provide the data as soon as possible and no later than within 14 days of receipt of the request by the School or the filing of the oral request. In both cases, the response must be sent to the School Data Protection Officer. If the data disclosure is refused, the head of the organizational unit designated for the data supply shall immediately notify the

School Data Protection Officer. If the request is denied, the requester shall be notified by electronic means within 15 days from the receipt of the request, in writing or, if the electronic mailing address is communicated in the request, by electronic means. If the data request relates to a large volume or to a large amount of data or the fulfilment of the data request involves a disproportionate use of the labour force involved in the core activities of the School, the 15-day response-deadline may be extended once by 15 days. In this case, the School Data Protection Officer shall inform the requester within 15 days of receiving the request.

(10) If the data request is unclear, the School Data Protection Officer will call upon the requester to clarify the claim.

(11) The School shall not be obliged to comply with requests:

(a) in those parts of the data request which are identical to the ones submitted by the same claimant within one year, provided that there has been no change in the data in the same dataset;

(b) if the claimant does not give their name, the identity of a non-natural person (if applicable), and the contact details to which any information and notification related to the data request may be sent to;

(12) The fulfilment of the request to access information of public interest cannot be denied on grounds that a non-Hungarian native requester formulates their request in their mother tongue or in another language they understand.

(13) If the law allows for the data controller to consider the denial of a request for information of public interest, the grounds for refusal must be interpreted narrowly and the fulfilment of a request for access to data of public interest may be denied only if the public interest underlying the refusal is stronger than the public interest in providing the data of public interest.

(14) Refused applications and the grounds for refusal must be recorded and the Authority must be informed about them by 31 January of each year. Maintaining records and fulfilling the obligation to provide information is the responsibility of the School Data Protection Officer.

(15) The data application shall be met in a manner that is comprehensible to the public and in the form requested as far as this may be accomplished by the School without disproportionate effort. If the School has already disclosed the requested information electronically, the claim may be fulfilled by indicating the public source containing the data. The data request cannot be rejected by claiming that it cannot be met in a comprehensible form.

(16) Where a document containing public interest data contains information that should not be shared with the claimant, the relevant data shall be redacted on the copy.

(17) Where the application relates to data produced by an institution or a Member State of the European Union, the School shall immediately consult the relevant institution or Member State of the European Union and inform the requester

thereof. From the moment of notification, the period up to the date of receipt of the response of the institution or Member State of the European Union concerned to the School shall not count towards the time limit for the provision of the reply.

(18) The requester may receive a copy of the document or part of the document containing the data. For the fulfilment of the request for information, up to the amount of the costs incurred in connection with it, a cost reimbursement can be determined, the amount of which the requester will be informed by the School Data Protection Officer before the fulfilment of the request. Based on that information, the requester shall declare whether they confirm the request within 30 days from receiving the information. The period from which the information is made until the date on which the claimant's statement to the data controller is received will not be included in the deadline for completing the request. If the claimant upholds their request, they must pay the reimbursement to the School within 15 days.

(19) If the volume of the document is significant, the request for a copy shall be fulfilled by the School within 15 days of the payment of the cost reimbursement and the requester will be informed within 15 days from receiving the request.

(20) For the fulfilment of the request for data, up to the amount of the costs incurred, the School may charge reimbursement. In determining the rate of reimbursement, the following cost elements may be taken into account:

(a) the cost of the medium containing the requested data,

(b) the cost of delivering the data medium to the requester, and

(c) if the fulfilment of the data request involves a disproportionate use of the labour force that is involved in the core activities of the School, the cost of labour input related to the fulfilment of the data request.

(21) In determining the rate of reimbursement, the School shall consider the provisions of the Government Decree on the extent of reimbursement for fulfilling demands for public interest data.

Budapest, 9th May 2018

Dr László LÁNG
Rector

Annex 1

Form for Registering data processing
Data processing
Data processing purpose
Legal basis (IBS regulation)
Data controller (organizational unit)
Person responsible (name, position, phone number)
Scope and number of data subjects
Type of data recorded
Data sources (data subject or other data processing)
Data transfer (Recipient, frequency, legal basis)
Place of data processing
Deadline for deleting data types

Annex 2

Form for registering combining data
Name of data processing actions combined
Purpose of combining data
Date and duration of combining data
Legal basis (IBS regulation)
Name, position organizational unit, phone number of the person combining the data
Scope and number of data subjects involved in combining data
Scope of data combined
Method of combining data (manual, computer, mixed)

Annex 3

Form for registering data transfer
Name, address and phone number of the body/person requesting the transfer
Purpose of the data request
Legal basis for the data request (or the declaration of the data subjects)
Date of the request
Data processing category
Organizational unit responsible for the data transfer
Data subjects
Scope of the data requested
Method of the data transfer

Annex 4

For for registering data transfer (based on student data record)
Name, address and phone number of the body/person requesting the transfer
Purpose of the data request
Legal basis for the data request (or the declaration of the Data Subjects)
Date of the request
Deadline of the data transfer
Frequency of the data transfer (recurring or single occurrence)
Data subjects
Scope of the data requested
Method of the data transfer