Rector's Directive No. 1/2013

On Data Protection and the Detailed and Uniform Data Management Regulation

Budapest, 2013

Version effective as of 31 January 2013

Directives on Data Protection and the Uniform Rules of Data Management

The Rector of the IBS International Business School (hereinafter referred to as the College) determines the order of data managements to be adhered to at the organisational units of the College in accordance with the Act CCIV of 2011 on national higher education (hereinafter referred to as the NHEA - National Higher Education Act), and pursuant to the Act CXII of 2011 on the right of information-related self-determination and the freedom of information (hereinafter referred to as the Data Protection Act) as follows.

Section I
Objective and Scope of Regulation

1. § (1) The objective of this regulation is to determine the statutory order of data management as to be pursued at the College, and to ensure that the requirements of the constitutional principles regarding data protection, information-related self-determination rights and data security be properly enforced.
(2) The scope of this regulation shall extend to all and any personal data management activities at the College – including the central units and all other organisational units.
(3) The provisions and objectives of this regulation are to be strictly respected and adhered to when the policies of the College considering document management and information security are being drawn up and applied.

Section II
Fundamental Concepts and Principles of Data Protection

Personal Data

2. § (1) For the purpose of these regulations the personal data shall mean all and any data connected with a particular natural person (hereinafter referred to as the person concerned) and any conclusions that may be drawn from any such data regarding the person concerned. Personal data shall retain this capacity in the course of data management as long as its connection with the person concerned remains restorable. A person may be deemed identifiable, in particular, when he or she – directly or indirectly – can be identified based on the name, identification number or code, or one or more factors characterising such a person's physical, physiological, mental, economic, cultural or social identity;
(2) Personal data mean identifying and descriptive data.
(3) Natural and artificial identifying data serve personalization of the person concerned. Natural identifying data are in particular the name, the mother's name, the place and date of birth, and the home address or the residential address. Artificial identification data are generated data based on mathematical or other algorithms, that may be assigned individually and exclusively to any natural person, in particular, the personal identification code, the National Insurance (NI) number, tax payer identification number, identity card number, passport number, college student identification number, identification number rendered to teachers and students by the body responsible for the functioning of the higher education information system (Section III/4 of Annex 3, NHEA).
(4) Descriptive data mean any other data considered relevant for the purpose of data management. Descriptive data that are not connected with a definite natural person (such as statistical data) are not considered as personal data.

3. § Data Management and Data Processing

4. § (1) Data management means any operation with personal data irrespective of the applied procedure (manual or computer based), in particular, data recording, data saving, data modification, data processing, data transmission, and the publication, archiving, filing, discarding or deleting of data.
(2) Data processing means the completion of technical tasks related to data management operations, regardless of the techniques and means used to carry out the operations, as well as of the place of application, provided that the technical tasks are done involving the data.

(3) The data processor can be an organisational unit or a third party concluding a contract with the College to perform the activities specified in Section (1***2***) on behalf of and following the directions of the data manager. If a third party is assigned with such tasks a written agreement on data processing shall be entered into. Such an agreement may be concluded also as a part of any other contracts.
(4) The data processor is not entitled to make any decision on the merits concerning data management, but may process the personal data obtained as directed by the data manager exclusively, and is not allowed to carry out any data processing for its own purposes, additionally it is obliged to store and retain the personal data as ordered by the data manager.

Restricted Purposes and Extent of Data Management

5. § (1) Personal data management is only allowed for a specific legal purpose, the exercise of rights or for the purpose of performing obligations, to the minimum extent and term as requisite for achieving the target. If the purpose of data management is ceased or the data management becomes otherwise illegal, the data must be deleted.
(2) Deletion means making the data unidentifiable so that they cannot be restored at all. The facts related to the deleting or discontinuation of data management shall be recorded. The detailed rules of data deletion are set forth in the Document Management Regulations of the College.

Section III

Rules of Data Management

6. § (1) Personal data can be managed by the College provided that

a) the person concerned consented to that in writing or in an electronically recorded form via the uniform central educational system operated for the purpose of research organisation and administration (hereinafter referred to as the Neptun system), or

b) it is ordered by the College's regulation under the law or under empowerment by the law.

(2) The College may manage data that are needed for the proper functioning of the institution, the exercise of rights and fulfilment of obligations by those enrolling to the college and by the actual students, for the exercise of rights by the institution as employer, for the exercise of rights and the performance of obligations and duties by the employees, for the organisation of training and research, for the maintenance of registers and records as required by the statutes, as well as for the evaluation and verification of eligibility for the allowances or favours granted by the statutes and the policies of the College.
(3) The College is entitled to manage the personal data related to employment, the establishment of benefits, allowances and duties and to the execution of the latter, for reasons of national security and for the purpose of managing the registers stipulated in the act on higher education, to the extent required for and bound to the purpose.
(4) The College shall manage the employees' personal data – unless otherwise ordered by a superior statute or the College's document management regulations – during the term of employment and after termination for further five years, while the students' personal data shall be managed during the term of the student's contract with the College and after termination for further eighty years.
(5) Before recording any personal data the person concerned shall be advised of the purpose of data management and whether the data provision is voluntary or obligatory. In the case of obligatory data provision the statute or the College's regulation requiring the data management shall be referred to.
(6) The employees performing data management at the organisational units of the College are obliged to treat the personal data becoming known to them confidentially as official secret. Such positions may be taken only by employees signing the declaration of confidentiality.

Data Management Register

7. § (1) A register shall be maintained on every data management activity at the College (Annex 1). This register shall be drawn up by the leader of each organisational unit responsible for data management. This power may be delegated by the head of the organisational unit. One original of the register shall be retained by the organisational unit executing the data management or data processing, while another original is held by the central administration of the College. The register shall be authenticated by the signature laid by the head of the data managing organisational unit.

(2) The register can also be maintained and saved in electronic format. Any such register can be authenticated by the qualified electronic signature of the authorised person.

(3) Within the framework of the central statutes and the regulations of the College the register shall regulate and document the major facts and circumstances related to data management in respect of each data management activity and in accordance with the constitutional principles of data protection. These are in particular the following:

a) name of data management,

b) purpose and designation,

c) statutory basis (act, the policy of the College),

d) managing person or unit (the organisational unit, the head thereof or the person responsible for data processing, with the name, office, and telephone number),

e) persons involved and number of persons concerned,

f) sphere of registered data type,

g) source of data (the person concerned or another data management),

h) data processing method (manual, computer based, combined),

i) frequent data management operations made to the data (saving, amendment, updating, sorting, systemising, etc.),

j) regular data transmission and typical individual data transmission

k) data security measures,

l) date of data saving and deleting.

(4) The data management registers are closely related to this regulation and form an integral part thereof.

(5) The data of the register shall be reviewed and amended by the head of the organisational unit executing the data management – especially, when the functions and authorities of the organisational unit are changed, and on the occasion of any other changes (such as a restructuring) to the organisational units. After the data management is terminated the register shall be properly retained as an archived file.

Rights of the Person Concerned

8. § (1) The person concerned may request information from the competent administrator about the data management on him or her, and may gain access to them. This data inspection shall be ensured so that no any data of any other persons may become known by the person concerned.

(2) As a response to the request the data manager shall provide the desired information on the data managed by him/her in writing within 15 days, additionally information shall also be provided on the purpose and legal grounds and the term of data management as well as on who and for what reason received the data.

(3) In accordance with Article 12 (1) of the Act CLV of 2009 on the protection of qualified data, the manager of the qualified data may refuse to provide information the person concerned is entitled to in accordance with the act on personal data protection if the public interest forming grounds for qualification was jeopardised by the provision of information to the person involved on the management of such person's personal data.

(4) In the case of changes in the data or if inaccurate recording of the data is noticed the person concerned may request the rectification or correcting of the data affected. The data manager is obliged to correct the inaccurate data within two business days.

(5) In the case of data management based on non-obligatory data provision the person concerned may request the deleting of his or her managed data without reasoning. The data must be deleted within two business days.

9. § The person concerned may turn to the head of the competent organisational unit (head of the centre) if his or her rights related to data management are offended. The Rector of the College shall settle any disputes between the person affected and the head of the organisational unit.

Section IV

Data Publication

10. § (1) Personal data may be disclosed to any third party within the framework of data transmission or publication.
(2) Data transmission shall mean the disclosure of data to a specific third party. Data transmission may be implemented by the inspection of data management or by the issuance of an excerpt.
(3) Data transmission to abroad shall mean the transfer of data to any (third) country outside the European Economic Area (EEA). Data transmission in the member states of the EEA shall be considered as inland data transmission.
(4) Disclosure shall mean making any data accessible to anyone.

Data transmission within the institution
11. § (1) The personal data managed by the College may be transferred within the organisational system of the College – to the extent and for a period of time required for the performance of any duties – to an organisational unit which needs any such data for the execution of duties specified in the relevant statutes or in the College's regulations or for the implementation of administrative or organisational duties for the purpose of contact keeping with the former students.
(2) Data transmission within the institution shall be recorded as a fact, provided that the data transmission is beyond the regular official practice of the College (specific data transmission). Specific data transmission shall mean especially any data transmission related to the changes to the duties of any individual organisational units or any data transmission involving at least 10% of the data files managed by a particular organisational unit.
(3) In addition to Subsection (3) above, the fact of data transmission within the institution shall be recorded, provided that it is expressly requested by the organisational unit either requesting or transferring the data.
(4) If the Subsections (2) and (3) are applied the following facts are to be recorded:
a) name of data management,
b) purpose of data transmission,
c) date of data transmission,
d) legal grounds (law or the College's regulation),
e) name, position, organisational unit, telephone number, e-mail address of the employee performing the data transmission,
f) sphere and number of persons involved in data transmission,
h) sphere of transmitted data,
i) data transmission method (manual, computer based or combined),
j) applied data security measures.
(5) The first original of the record shall be retained at the place of data management, while the second original shall be forwarded to the Legal Office of the College for the purpose of filing as an attachment to this regulation. The records shall be retained for a period of ten years.
(6) In the cases set forth in Subsections (2) and (3) the data transmissions are not required to be recorded, if the fact of the same is put down in writing otherwise in an authentic (filed) manner, provided that the items specified in the Subsections (4) a) to j) are included in any such document.

Data transmission upon an external request
12. § (1) Any requests for the disclosure or publication of any data received from a body or private person outside the College may be fulfilled solely when the person concerned consents the disclosure or publication of his or her data in writing or in a format electronically recorded. Any such consents may be granted by the person concerned also in advance, and this consent may be applicable for a period of time or for the specific sphere of the requesting body.

(2) Regardless of the declaration by the person concerned the data transmissions must be fulfilled in the following cases:
a) if the data are required for the performance of duties related to the institution maintaining management of the College by the managing body,
b) if data are required by the court, the police, the public prosecutor's office, the bailiff or the public administration bodies for the judgement of certain matters, and
c) if any data are required by the national security agencies,
d) relevant to all data transferred by the body responsible for the operation of the higher educational information system,
e) the requests by the Student Loan Centre in respect of data concerning the studies,
f) if called for by the law with the exception of Subsections a) to f).
(3) The data request must not be fulfilled if the lawfulness is impossible to be established – out of consideration for the deficient or incomplete data content of a data request or consent by the person concerned, or any other circumstances.
(4) The head of the organisational unit involved shall notify the Rector of the College of any data requests by the national security agencies. The Rector may resort to a complaint with non-deferring effect addressed to the competent minister against any such requests.
(5) The person concerned, or any other persons or organisations may not be notified of the request received from the national security agencies, or of data relevant to data inspection – including the fact of request or inspection – or of the measures taken.
(6) The facts and circumstances relevant to the data provision fulfilled upon the request are to be documented by taking records. Any such records shall include the following:
a) name, postal address and telephone number of the body or person initiating the request,
b) purpose or objective of the data request,
c) statutory grounds for the data request, or the declaration of consent by the person concerned,
d) date of data request,
e) name of data management serving as basis for the data provision,
f) name of the organisational unit implementing the data provision,
g) sphere of persons concerned,
h) sphere of data requested,
i) method of data transmission,
j) data security measures applied.
(7) The first original of the records on the data request shall be retained by the responsible data manager, while the second original shall be retained by the Legal Office of the College. The records shall be retained for a period of ten years.
(8) No recording of data transmissions is needed, the fact of which is documented otherwise in an authentic manner, provided that the document includes the items specified in the Subsections a) to j) (6) above. Therefore no recording of the requests are required when the request is received in writing, the request is filed by the competent organisational unit, and the data transmission is implemented in a filed written document.
(9) The fact of data transmissions shall be recorded so that the organisational unit can establish the data transmissions relevant to a particular person concerned and can meet the requirement of information provision as set forth in Subsection 8 (2) above (data transmission register).

Data transmission to abroad

13. § (1) In the case of data management when data transmission to abroad or to any member state of the EEA is to be counted with, the attention of the persons concerned shall be drawn to this circumstance prior to the data recording. In the lack of a written consent by the person concerned no personal data may be transferred to abroad unless ordered by the law, provided that in the country involved the data security is ensured properly.
(2) No data request received from abroad may be fulfilled the lawfulness of which is impossible to be established – out of consideration for the deficiency of data request or incompleteness of the consent granted by the person concerned.
(3) The facts and circumstances relevant to data provision to abroad are to be documented by taking records. Any such records shall include the following:

a) name, postal address and telephone number of addressee requesting data transmission,
b) purpose and objective of data transmission,
c) statutory grounds for the data transmission, or the declaration of consent by the person concerned,
d) date of data transmission,
e) name of the organisational unit performing the data transmission,
f) sphere of persons involved,
h) sphere of transmitted data,
i) data transmission method

(4) The first original of the records on data transmission to abroad shall be retained at the place of data management, while the second original shall be retained by the Legal Office of the College. The records shall be retained for a period of ten years.

(5) No recording of data transmissions is needed, the fact of which is documented otherwise in an authentic manner, provided that the document includes the items specified in the Subsections a) to h) (3) above. Therefore no recording of the requests are required in particular when the request is received in writing, the request is filed by the competent organisational unit, and the data transmission is implemented in a filed written document.

Order of data transmission

14. § (1) If the conditions for data transmission obviously exist, the person in charge of data management shall perform the data transmission in accordance with the provisions set forth in Subsections 11 to 13.

(2) Should any doubt as for the rightfulness of data transmission emerge, the official in charge of data management shall notify the responsible manager of the organisation performing the data management without delay about the receipt of request for data transmission under Subsections 11 to 13. The head of the organisational unit shall investigate relying on the available information whether the conditions for the data transmission exist or the request is feasible and if necessary further information is provided.

(3) In the case of the provisions set forth in Subsection (2) the head of the organisational unit receiving the request shall make a decision on the fulfilment of requests, if necessary, respecting the position taken by the designated responsible body or person – within 15 business days. The data requesting party may submit to the secretary general a complaint against the decision in writing within 15 days and the secretary general shall decide, within 15 days, on whether the data can be transmitted.
(6) Should the conditions of data transmission exist, the data shall be provided to the requesting body. The costs related to the data transfer shall be borne by the requesting body. The head of the organisational unit carrying out the data management shall arrange for and ensure the taking of the records on the data transfer.

Publication of Personal data
15. § Publication of personal data managed at the College shall be forbidden – unless ordered by law or consented by the person concerned. This prohibition shall not apply to the display of names and examination results in the building in respect of students taking the entrance examination or students taking any examinations conforming the practice at the College. The statistical data relevant to the College – also based on personal data – can be published without restrictions.

Section V

Data security rules
16. § (1) Data security rules and measures are intended to protect the data and data carriers and prevent any unauthorised access thereto, or any unauthorised changes, transfer, publication, deleting or demolition, as well as to protect them against any accidental destruction and damaging, additionally against becoming inaccessible due to changes to the applied technology.
(2) To ensure the security of personal data all and any necessary measures must be taken both in the case of manually managed and those saved and processed by the computer. The individual data security measures are recorded in the data management register.

Data stored on computer (automated data processing)
17. § (1) In the course of automated processing of the personal data the College shall ensure
a) that any unauthorised data entry shall be prevented,
b) the use of the automatic data processing system by unauthorised persons, with the use of data transmission devices,
c) the verifiability of which personal data were entered in the automatic data processing system by whom and when, and to which bodies the personal data were or can be transmitted by means of data transmission devices,
d) the restoration of installed systems in the case of a breakdown of the systems and that any mistakes or faults that may emerge shall be reported.
(2) When the measures intended to ensure data security are determined and applied the, at all time, actual advancements of technology shall be respected. From among the possible data management solutions the one, which ensures a higher standard of protection to personal data, shall be selected, unless they would entail disproportionately great difficulties to the data manager.

(3) The Information security regulations of the College stipulate the detailed rules on data security.

Manually managed data

18. § (1) For the security of manually managed personal data the following measures are to be implemented (see further details in the Document management regulations):

a) *Fire and property protection:* Documents to be managed in the archives are to be stored in a securely locked and dry room, where fire and property protection alarm system is also installed.

b) *Access control:* Only the authorised officials in charge may access to the documents in continuously active use. Personnel, payroll and employment related documents are to be stored in a metal-plate cabinet, while the study contract documents are to be stored separately, in a securely locking room, in locking metal-plate cabinets.

c) *Archiving:* Archiving of documents shall take place in accordance with the College' document management and rejecting regulations, following the archiving schedule.

Section VI
Data protection controlling system

19. § (1) Observance of regulations on data protection, in particular, the specifications of this regulation are continuously controlled by the head of the organisational units performing data management and data processing.

(2) If any acts against laws is detected or found, the head of the organisational unit shall take steps and actions to eliminate such circumstances without delay.

Miscellaneous and Closing Provisions

20. § (1) This regulation in a uniform structure shall enter into force on 31 January in 2013, in the form of the Rector's Directive. When this regulations becomes effective all other internal rules and regulations issued in this subject matter beforehand shall become void.

(2) This regulations shall be applied in the scope of data managed by the Students' Representation for which the leaders of the IBS Student Self-Government shall be responsible. The IBS Student Self-Government shall be obliged to accept jurisdiction of this regulation, and accordingly, the Chairman of the Self-Government shall acknowledge understanding of the content of this regulation and the acceptance as binding to the IBS Student Self-Government by signing the clause of the regulation.

Budapest, 30 January 2013

IBS International Business School
Dr. László Láng
Rector

Clause:

This data protection regulation in uniform structure applicable to the institution shall be accepted by the IBS Student Self-Government as binding and governing relevant also to the data collected and/or managed in the scope of its functions, and the provisions of the regulation shall be adhered to accordingly – it the course of its actions the IBS Student Self-Government shall cooperate with the leaders and organisational units of the College involved in data protection.

Budapest, 30 January 2013

IBS International Business School
Chairman of the IBS Student Self-Government as legal representative

Annex 1

Data management register

Name of Data management:
1. Organisational unit
2. Purpose of data management
3. Statutory basis of data management:
4. Responsible leader of data management:
5. Name and position of persons authorised to access:

6. Sphere and number of persons concerned:	**……..persons**	
7. Sphere of data registered:		
	Identifying data	**Descriptive data**
8. Data sources:	**Identifying data**	**Descriptive data**
9. Data processing method	**Manual processing**	**Detailed description**
	Mechanical processing	
	Combined processing	

10. Place of data processing ***(To be filled in only if differs from the organisational unit responsible for data management.)***

11. Data management operations	**Data collecting and recording**
	Data storage
	Systematizing
	Sorting
	Transmission
	Publication
	Deletion
	Other operations: ……..