M U N I

Masaryk University Directive No. 1/2018

PERSONAL DATA PROCESSING AND PROTECTION

(in the version effective from 15 June 2020)

In accordance with Section 10(1) of Act No. 111/1998 Coll., On Higher Education Institutions and on Modification and Amendment of Other Acts (Higher Education Act), as later amended (hereinafter referred to as the "Act"), I issue this Directive:

Section 1

Subject of Regulation

(1) The Directive sets forth the principles, rules and processes of personal data processing carried out by Masaryk University (hereinafter referred to as the "University").

(2) The subject hereof is the personal data processing where the University is in the position of a data controller or processor.

(3) The Directive is based on the Regulation (EU) 2016/679 of the European Parliament and of the Council 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 referred to as the "GDPR"), and Act No. 110/2019 Coll., on Personal Data Processing.

Section 2

Definitions

(1) For the purposes hereof, the terms "personal data", "personal data processing", "controller", "processor", "third party", "'filing system", "consent", "personal data breach", and other related terms shall be used in the sense of definitions under Article 4 of the GDPR.

(2) For the purposes hereof:

a) "person in charge" means a person mentioned in Sections 3 and 4;

b) "data protection officer" means a person authorized with the protection of personal data;

c) "Register" means the register of data processing activities under Section 14(b).

Section 3

Persons in Charge – Management Staff

(1) The Rector is the highest management level under the GDPR.

(2) The bursar is responsible to the Rector for the compliance with principles, rules and procedures of personal data processing during the execution of his/her authority under the Organizational Regulations.

(3) The vice-rector is responsible to the Rector for the compliance with principles, rules and procedures of personal data processing during the execution of his/her authority under the Organizational Regulations.

(4) The dean is responsible to the Rector for the compliance with principles, rules and procedures of personal data processing during the execution of the faculty's

activities under Section 24 of the Act, Section 15 of the Statutes, and internal and other regulations of the University.

(5) The director of a University institute is responsible to the Rector for the compliance with principles, rules and procedures of personal data processing during the execution of the institute's activities under Section 16 of the Statutes, organizational regulations of the University institute, and internal and other regulations of the University.

(6) The director of a University facility is responsible to the Rector for the compliance with principles, rules and procedures of personal data processing during the execution of activities under Section 17 of the Statutes, organizational regulations of the University facility, and internal and other regulations of the University.

Section 4

Person in Charge – Guarantor

(1) The Guarantor is a person in charge in place of the persons stated in Section 3, responsible for the compliance with principles, rules and procedures of personal data processing in the extent entrusted to them.

(2) The head of a research task is a guarantor under MU Directive No. 6/2013 – Research Data. In other cases, the guarantor is appointed through the Register by:

a) the Rector in case of processing of personal data with University-wide impact or in case there is no agreement under clause e);

b) director of the Institute of Computer Science for the processing of personal data in information systems administered by the Institute of Computer Science;

c) head of the Computer Systems Unit of the Faculty of Informatics for the processing of personal data in information systems administered by the Computer Systems Unit of the Faculty of Informatics;

d) head of a University constituent part for the processing of personal data by that constituent part;

e) head of a University constituent part appointed by agreement for joint processing of personal data by more constituent parts.

Section 5

Persons Authorized to Access Personal Data

(1) Besides a person in charge, personal data may be processed by:

a) a person authorized by the person in charge to access personal data or to fulfil an assigned working task requiring access to personal data;

b) a person superior to persons mentioned in clause a);

c) a person determined by the administrator of an MU IT constituent (within the meaning of MU Directive No. 9/2017 – Administration of Information Technology) to provide services to the MU IT constituent through which personal data are processed.

(2) The person in charge is obliged to ensure that persons under subsection 1(a) and (b) are informed of personal data protection obligations ensuing from legal regulations and this Directive.

(3) The administrator of an MU IT constituent (within the meaning of MU Directive No. 9/2017 – Administration of Information Technology) is obliged to ensure that the person under subsection 1(c) is informed of personal data protection obligations ensuing from legal regulations and this Directive.

Section 6

Obligation of Confidentiality

(1) Anyone who got access to personal data processed under Section 1(2) or to security measures adopted for the protection of personal data is obliged to maintain confidentiality thereof except for cases where it is excluded by the law or by an obligation imposed by such law.

(2) The obligation under subsection 1 shall survive the termination of employment, study or another relation with the University.

(3) A person may be released from the obligation under subsection 1 by the Rector.

Section 7

Personal Data Processing Documentation

(1) Upon a request of the superior or the data protection officer, the person in charge is obliged to prove the compliance with principles, rules and procedures of personal data processing.

(2) For the purpose of meeting the obligation under subsection 1, the person in charge is obliged to provide documentation proving:

a) legal grounds for personal data processing;

b) purpose of personal data processing;

c) method of personal data processing;

d) security measures to reduce the risks associated with personal data processing; and

e) legal acts associated with the processing of personal data (e.g. contracts, consents, documents on the settlement of complaints and motions, etc.).

(3) In case personal data are transferred to third parties for another purpose than the fulfilment of a statutory obligation, the person in charge is obliged to assess and provide documentation proving that the third party is capable of complying with legal regulations as well as internal and other regulations of the University when protecting personal data.

(4) The person in charge of the camera system operation is obliged to provide the following documents in addition to obligations under subsections 2 and 3:

a) location of the cameras;

b) retention periods for camera recordings;

c) management of access to camera recordings;

d) manner of informing data subjects of the camera system operation.

(5) The person in charge is obliged to ensure that the documentation under subsections 2, 3 and 4 is available for at least five years of the termination of personal data processing.

Section 8

Personal Data Security

(1) Everyone is obliged to act so as to prevent breach of obligations in personal data processing which ensue from legal regulations and this Directive.

(2) For the purpose of personal data security, everyone is obliged to:

a) protect data carriers and deeds containing personal data from unauthorized access by locking them in suitable places at the University workplaces or secure them in another suitable manner including encoding;

b) secure computers and other technical devices through which personal data are processed from unauthorized access;

c) in cases which are not governed by MU Directive No. 2/2016 – MU Document Management Rules to erase personal data in relation to which the purpose or legal grounds for processing has expired.

Section 9

Personal Data Processing as Part of Instruction

(1) In case personal data processing is part of the instruction, performance of study duties or preparation of diploma or degree theses, the relevant teacher or supervisor is obliged to inform the student of personal data protection obligations ensuing from legal regulations and this Directive. Personal data processing that is part of the instruction, performance of study duties or preparation of diploma or degree theses should only be carried out in the least extent necessary.

(2) The relevant teacher or supervisor under subsection 1 is obliged to assess the risk of impact of personal data processing upon the rights of the data subjects and notify the person in charge of the personal data processing and the associated risk level.

Section 10

Publication of Personal Data of Employees, Students and Other Persons

(1) The University makes public the following personal data of students active in the University's autonomous academic or advisory bodies, and of employees:

a) first name and surname;

b) degrees;

c) photograph;

d) job title at the University;

e) place in the University organizational structure;

f) offices held at the University;

g) contact details at the University;

h) curriculum vitae;

i) history of academic qualifications;

j) contribution to creative activities of the University;

k) information about publications;

l) teaching activities at the University;

m) personal website address;

n) university identification number.

(2) The data subject may define the scope of the published data under subsection 1(c), (h), and (m) or decide on non-disclosure.

(3) The Rector is entitled to decide on the publication of other personal data of academic officers and heads of University constituent parts.

(4) The University publishes the first name, surname and institutional affiliation of members of autonomous academic or advisory bodies; the chair of the relevant body decides on the publication of other personal data of persons who are not employees or students of the University.

Section 11

Position of Data Protection Officer

(1) The data protection officer is appointed and dismissed by the Rector.

(2) The data protection officer is an employee of the University and reports directly to the Rector.

(3) Information about the data protection officer is stated in the public part of the University website.

Section 12

Tasks of Data Protection Officer

Besides tasks stipulated by legal regulations, the data protection officer:

a) if required by a legal regulation, upon prior consultation with the person in charge notifies the Office for Personal Data Protection of a personal data breach, and notifies the data subject of a personal data breach;

b) accepts notifications under Section 13(2)(d) and (e) and gives opinions thereof;

c) accepts requests, complaints and other motions of data subjects concerning personal data processing and refers them together with his/her opinion to persons in charge;

d) alerts persons in charge of a real or impending breach of obligations in personal data processing and proposes solutions;

e) recommends adopting measures for the protection of personal data to persons in charge;

f) negotiates with the Rector, heads of the University constituent parts, and persons in charge the personal data processing with the risk to rights and freedoms of the data subject;

g) issues general recommendations for personal data processing through the IS MU Bureau;

h) in case the University is a personal data processor, informs the data controller of a real or impending breach of obligations in personal data processing;

i) reports suspicion of a cybersecurity incident to CSIRT MU (within the meaning of Directive No. 9/2017 – Administration of Information Technology).

Section 13

Obligations Towards Data Protection Officer

(1) Everyone is obliged to:

a) provide assistance to the data protection officer in the performance of his/her tasks under legal regulations and this Directive;

b) report a data breach (under Article 4(12) GDPR) through a form "Incident Report" in the IS MU;

c) refer a request, complaint or motion concerning the personal data processing received from a data subject to the data protection officer.

(2) Person in charge is obliged to:

a) discuss alerts and proposals under Section 12(d) with the data protection officer;

b) discuss recommendations under Section 12(e) with the data protection officer;

c) in case he/she does not follow proposals or recommendations of the data protection officer under Section 12(d) and (e), provide written explanation and reasoning;

d) using the Register, notify the data protection officer of the commencement, change or termination of personal data processing;

e) using the Register, notify the data protection officer of the personal data transfer to a third party;

f) discuss with the data protection officer the intention to transfer personal data for processing outside the European Economic Area;

g) discuss with the data protection officer the intention to process personal data with the risk to rights and freedoms of the data subjects (under Article 35(1) GDPR);

h) in case personal data are to be processed for another purpose than that for which they were obtained, and the purpose is not research activities, to discuss with the data protection officer the intention to process personal data for another purpose than that for which they were obtained (under Article 5(1)(b) GDPR).

Section 14

Records of Processing Activities

Records of personal data processing activities (under Article 30 GDPR):

a) for the processing of personal data carried out in the IS MU shall be filed in section "Information on personal data processing activities" in the IS MU. The administrator of such records is the Computer Systems Unit at the Faculty of Informatics;

b) for other processing of personal data shall be filed in the Register. The administrator of the Register is the Institute of Computer Science.

Section 15

Final Provisions

(1) This Directive repeals MU Directive No. 1/2018 – Personal Data Processing and Protection of 31 January 2018 effective from 1 February 2018.

(2) This Directive repeals MU Order No. 4/2018 – Procedure in the Case of Data Breach of 16 October 2018 effective from 18 October 2018.

(3) This Directive repeals MU Measure No. 4/2018 – Personal Data Processing and Protection of 15 February 2018 effective from 15 February 2018.

(4) I authorize the Legal Office of the MU Rector's Office to interpret the individual provisions hereof.

(5) This Directive is part of the methodology management "Legislation and Legal Activities".

(6) The compliance with this Directive shall be inspected by the data protection officer.

(7) This Directive shall enter into force on the day of its execution.

(8) This Directive shall enter into effect on 15 June 2020.

electronic signature

Martin Bareš
Rector