SLEZSKÁ
UNIVERZITA
V OPAVĚ

Rector's Directive No. 10/2018

Personal Data Protection and Processing

Published in Opava, July 2018

SLEZSKÁ UNIVERZITA V OPAVĚ

Rector's Directive No. 10/2018

Personal Data Protection and Processing

Article 1

Basic provisions

1) This Directive sets out the principles, rules and procedures for the processing of personal data within the Silesian University in Opava (hereinafter referred to as "the University"), establishes the responsibilities of persons ensuring the protection of personal data at the University, and defines the rights and obligations of employees, students, and other natural and legal persons involved in activities related to the processing of such data.

2) This Directive is based on Regulation (EU) No 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), (the "Regulation"), and supplements and elaborates the obligations given by the generally applicable legislation to the conditions of the University.

Article 2

Interpretation of selected related terms

1) "Personal data" means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable natural person is 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, a network identifier or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2) "Processing of personal data" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated processes, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other disclosure, alignment or combination,

restriction, erasure or destruction.

3) "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or estimate aspects relating to their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

4) "Pseudonymisation" means the processing of personal data so that they can no longer be attributed to a specific data subject without the use of additional information, provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that it is not attributed to an identified or identifiable natural person.

5) "Record" means any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or disaggregated by function or geography.

6) "Controller" means the entity which alone or jointly with others determines the purposes and means of the processing of personal data, in this case the University;

7) "Processor" means a natural or legal person, public authority, agency or other body which processes personal data for the controller;

8) "Recipient" means the natural or legal person, public authority, agency or other body to which personal data are disclosed (whether or not a third party), except for public authorities which may receive personal data in the context of a special investigation in accordance with applicable legislation.

9) "Third party" means a natural or legal person, public authority, agency or other entity which is not the data subject, controller, processor or a person directly under the control of the controller or processor who is authorised to process personal data.

10) "Consent" of the data subject is any free, specific, informed and unambiguous expression of will by which the data subject gives their consent to the processing of their personal data, whether by declaration or other manifest acknowledgement.

11) "Personal data breach" means a breach that results in the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

12) "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which provide unique information about the physiology or health of that natural person and which result, in particular, from the analysis of a biological sample of the natural person concerned.

13) "Biometric data" means personal data resulting from specific technical processing which relate to physical, physiological or behavioural characteristics of a natural person which allow or confirm unique identification. This includes, for example, facial images or dactyloscopic data.

14) "Health data" means personal data relating to the physical or mental health of a natural person, including data relating to the provision of health services, which are indicative of their state of health.

15) "Coordinator" means an employee of a faculty, university institute or Rector's office who is responsible for coordinating the processing of personal data.

Article 3

Employee responsibility

1) The University is the entity responsible for the processing of personal data in the context of the University's activities, both as a controller and as a processor. The University's statutory body, i.e. the Rector, has the primary responsibility for compliance with the principles, rules and procedures for processing personal data.

2) The Deans of faculties, Directors of university institutes, Heads of university departments and Vice-Rectors and the Bursar are responsible for compliance with the principles, rules and procedures for the handling of personal data at individual units within the scope of their authority at the Rector's Office.

3) The Deans of the faculties and the Director of the university institute are obliged to designate a coordinator whose duties are specified in this Directive and in the job description; they are obliged to inform the Data Protection Officer of this fact without delay.

4) Senior staff at all levels of management are responsible for creating the conditions, setting up the appropriate working procedures and monitoring compliance with them on an ongoing basis, within the limits of their authority.

5) The security of information systems is the responsibility of the administrator of the information system in cooperation with the author, supplier or operator (hereinafter referred to as the "provider") of the information system. The administrator of the information system is also responsible for setting user access rights to the information system in accordance with the internal standards of the University. The cooperation between the information system administrator and the information system provider is specified in a service contract. The processing of personal data by the provider shall be governed by a contract or other legal act concluded to the extent provided for in Article 28(3)(a) to (h) of the Regulation.

6) All employees are obliged to comply with the principles, rules and procedures for the processing of personal data in their area of activity.

Article 4

Data Protection Officer

1) The Data Protection Officer is an employee of the University who is appointed and dismissed by the Rector. The function of the Data Protection Officer may be performed concurrently with the performance of other tasks and duties, none of which may lead to a conflict of interest with the performance of the function of the Data Protection Officer.

2) The contact details of the Data Protection Officer are provided in the public section of the University's website, including information on how and in what form information is provided to data subjects.

3) The Data Protection Officer shall be bound by confidentiality in connection with the performance of their tasks. The details of the obligation of confidentiality may be regulated by a separate agreement.

4) In particular, the Data Protection Officer performs the following tasks:

   a) provides information and advice to students and University staff who process personal data on their obligations under this Directive, the Regulation and other generally binding data protection legislation;

   b) monitors compliance with this Directive, the Regulation, other generally binding data protection legislation and the University's internal rules and standards, including the allocation of responsibilities, awareness raising and training of staff involved in processing operations and related audits;

   c) supervises the implementation of the personal data protection and processing;

   d) provides advice and technical assistance on the data protection impact assessment and monitors its implementation, upon request;

   e) after prior consultation with the persons referred to in Article 3, paragraph 2), reports personal data breaches to the Office for Personal Data Protection (hereinafter referred to as the "OPDP") and reports personal data breaches to the data subject;

   f) cooperates and communicates with the OPDP, acts as a contact point for the OPDP in matters relating to the processing of personal data;

   g) receives proposals from University employees to initiate new or change existing processing of personal data and takes a position on such proposals;

   h) communicates with data subjects, who may contact them on all matters relating to the processing of their personal data and the exercise of their rights;

   i) performs other tasks arising from their position, from regulations, law or other generally binding legal regulations or arising from this Directive and other internal regulations and standards of the University;

   j) performs the activities of the coordinator for the protection and processing of personal data within the University Rector's Office.

5) The Data Protection Officer shall oversee the operation of the University's data processing register referred to in Article 9.

6) In carrying out their tasks, the Data Protection Officer shall take into account the risks associated with the processing activities, taking into account the nature, scope, context and purposes of the processing.

7) If the Data Protection Officer becomes aware that there is a risk of a breach of the rules on the protection of personal data arising from the Regulation, the Act or this Directive, or if a breach is detected, the Data Protection Officer shall draw the attention of the competent person referred to in Article 3(2) and the coordinator designated by them to this fact and recommend in writing that the defective or risky situation be remedied. That person or coordinator shall discuss the facts with the Data Protection Officer within a reasonable period of time and, if the recommendation is found to be justified, shall ensure that the situation is remedied, including the adoption of measures to prevent its recurrence. If the recommendation of the Data Protection Officer is not accepted, this must be justified in writing, including giving specific reasons. In this case, the Officer will refer the case in question, including all documentation, to the Rector for a decision on remediation or acceptance of the risk.

8) The Data Protection Officer shall be obliged to initiate general or individual data protection measures to the persons referred to in Article 3(2) whenever:

a) they identify a threat of a breach or a breach of the rules based on their findings;
b) this is be appropriate in the context of the generalisation of data protection practice.

9) The provisions of paragraph 7 shall be without prejudice to the obligation of the Data Protection Officer, after prior consultation with the persons referred to in Article 3(2), to report a personal data breach to the OPDP and the data subject pursuant to paragraph 4(e).

Article 5

Authorisation to process personal data

1) The following are authorised to process personal data:

a) employees during the performance of their job function and according to their job description;
b) staff superior to the persons referred to in (a) in terms of organisation or methodology;
c) employees who provide organisational, functional and technical administration of the relevant data processing (generally analysts, programmers, system and network administrators, etc.);
d) students authorised to use this personal data to carry out their tasks.

2) Before starting an activity requiring authorisation to process personal data, the immediate superior is obliged to familiarise the employee with the principles, rules and procedures for processing personal data within the scope of activities according to their classification (see the model in Appendix 1).

3) The persons referred to in paragraph 1 shall always be obliged to process personal data only to the extent necessary for their activities.

4) The persons referred to in paragraph 1 shall be obliged to maintain the confidentiality of personal data and security measures the disclosure of which would jeopardise the security of personal data. The details of the obligation of confidentiality may be regulated by a separate agreement.

5) If an employee is required to handle personal data and they do not meet any of the conditions set out in paragraph 1), the employee must notify their immediate superior in advance.

6) In cases where a student processes personal data as part of their study obligations or final thesis, the employee – teacher who assigns such work is responsible for familiarizing them with the obligations in accordance with this Directive.

Article 6

Principles and rules for processing personal data

1) Personal data must be:

a) processed in a lawful, fair and transparent manner in relation to the data subject;
b) collected for specific, explicitly stated and legitimate purposes and may not be further processed in a way that is incompatible with those purposes;

c) proportionate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

d) accurate and updated where necessary. All reasonable steps shall be taken to ensure that personal data which are inaccurate with regard to the purposes for which they are processed are erased or rectified without delay;

e) stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

f) processed in a manner that ensures appropriate security of personal data, including protection by appropriate technical or organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2) Personal data may only be processed to the appropriate extent and in the event that:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes (see Appendix 2); or

b) the processing is necessary for the performance of a contract to which the data subject is a party or for the performance of pre-contractual measures taken at the request of the data subject; or

c) the processing is in accordance with applicable generally binding legal provisions and is necessary for compliance with a legal obligation to which the controller is subject; or

d) the processing is necessary for the protection of the vital interests of the data subject or of another natural person; or

e) the processing is in accordance with the applicable generally binding legal provisions necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f) the processing is necessary for the purposes of the legitimate interests of the relevant controller or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data, in particular where the data subject is a child (except for processing of personal data carried out by the University where the University acts as a public authority in matters entrusted to it by law).

3) Consent to the processing of personal data given by individual data subjects must be immediately forwarded by the employee who has requested it from the data subject in the course of their work to the coordinator, who will ensure that it is stored or forwarded to the relevant department.

4) Consent to the processing of personal data given by individual data subjects shall be stored according to whether it is consent given by:

– an employee – in the personnel file,

– a job applicant – in the records of the recruitment procedure documentation in the electronic file system,

– a student, an applicant, a graduate – in the folder of the applicant, student, graduate,

– a person interested in studying in a LLL programme or an internationally recognised course – with the application form,

– another person – in the relevant file documentation.

5) Where processing for a purpose other than that for which the personal data were collected is not

based on the data subject's consent or on applicable generally binding legal provisions, it must be verified in advance whether the processing for the other purpose is compatible with the purposes for which the personal data were originally collected. In doing so, account shall be taken of:

a) the link between the purposes for which the personal data were collected and the purposes of the intended further processing;
b) the circumstances in which the personal data were collected, in particular as regards the relationship between the data subjects and the University;
c) the nature of the personal data, in particular whether it is a special category of personal data or personal data relating to criminal convictions and offences;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Processing of special categories of personal data

1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person and data concerning the health or sex life or sexual orientation of a natural person is prohibited. Exceptions to this prohibition are set out in Article 9 of the Regulation; in the University's cases, the exception applies in particular to processing:

   a) health data in the personal records of employees and students, provided that such data have been voluntarily provided by the data subject to the said records and are kept for their benefit (e.g. they affect admission to studies, the provision of services to persons with specific requirements, accommodation in dormitories or the calculation of their tax liability or other statutory benefits);
   b) data on membership of trade unions operating at the University contained in the personal and payroll records of employees, provided that they have been voluntarily submitted by the data subject to the said records and are used for the payment of membership fees or other benefits, including the accounting of such payments,
   c) biometric data which allow direct identification or authentication of the data subject,
   d) data processed for project/research purposes.

2) The processing of the data defined in paragraph 1 may only take place on the basis of the data subject's explicit consent. This consent must be given in writing, signed by the data subject and must make it clear to which data it relates, for what purpose, for what period and by whom and that the data subject has been informed in advance of their rights (see model in Appendix 2). The existence of this consent must be documented throughout the processing.

Article 8

Security of personal data

1) Writings and technical media (including external, portable, etc.) containing personal data must be kept only:

   a) in securely lockable cabinets or drawers in University workplaces,

   b) in designated rooms where only authorised staff have access,

   c) in other secure locations determined by the characteristics of the personal data processing concerned.

2) Employees processing personal data are obliged to ensure that the workplace is organised in an appropriate manner so that other persons are not able to view the personal data processed in written or electronic form when performing their activities.

3) Computers and other technical means on which data containing personal data are stored must always be secured by the user against free access by unauthorised persons, usually by means of passwords, encryption or locking, even when leaving the workplace for a short period of time.

4) Personal data may only be transferred to other persons by secure means, i.e. primarily by:

   - password-protected files sent as an email attachment, whereby the password must be communicated to the recipient separately (verbally, by text message, etc.),
   - the University's secure storage, i.e. shared drives or the cloud environment box.slu.cz or MS Office 365.

   It is only possible to transmit personal data in the text of an e-mail message if the message is encrypted with a personal certificate.

5) Copies of personal data for backup purposes shall be made on the University's technical means in accordance with the operating rules laid down for individual data processing and stored in accordance with paragraph 1, and on principle shall always be stored in a different room from the original data.

6) In the event that a University employee becomes aware or suspects that a personal data breach may have occurred or has occurred, they shall immediately notify the persons referred to in Article 3(2) or the Coordinator or the Data Protection Officer.

7) The notification of personal data breaches to the OPDP and the notification of personal data breaches to the data subject shall be carried out by the Data Protection Officer after prior consultation with the persons referred to in Article 3(2).

Article 9

Register of the processing of personal data

1) In order to provide an overview of the processing of personal data at the University, an electronic register of the processing of personal data at the University (hereinafter referred to as the "register") is hereby established. The Data Protection Officer shall be responsible for entering data into the register and keeping it up to date. The operation of the register is delegated to the Centre for Information Technology (hereinafter referred to as "CIT"). The Head of CIT is responsible for the operation of the register.

2) At minimum, the data listed in Appendix 3 shall be recorded in the register. Every employee of the University has the right to consult the register.

3) The input data shall be entered in the register when it is established on the basis of the results of the analysis carried out by internal audit after verification by the persons referred to in Article 3(2). In the event that additional activities involving the processing of personal data arise at individual units or a change is made to the existing method of processing personal data, the coordinators are obliged to request a binding opinion from the Data Protection Officer on the intention of such a change in the form of a Notification of New Activities/Change of Activities (see Appendix 3).

4) The proposed change to the processing of personal data pursuant to paragraph 3 may only be implemented after the consent of the Data Protection Officer to the change has been obtained. If the Data Protection Officer does not agree to the new processing or to the processing change, they shall discuss this with the relevant senior employee referred to in Article 3(2) and propose an appropriate solution in the context of the consultation.

Article 10

Disclosure of personal data

1) Disclosure of personal data means making it available to persons or groups of persons not specifically identified, in particular by mass media, other public communication or as part of a public list (e.g. in the public section of the University's website).

2) Personal data may be disclosed in this way to the maximum extent of:

   a) name, surname, titles;

   b) job classification at the University and position in the university's organisational structure, positions held at the University;

   c) contact details in relation to the University (addresses of departments, telephone and fax numbers, e-mail addresses);

   d) CV and academic qualifications;

   e) photographs;

   f) participation in individual forms of creative activities of the University, information on publications;

   g) teaching carried out at the university;

   h) academic websites (i.e. websites of university staff and students related to their

academic and/or study activities at the university);

i) where applicable, other data requested by the data subject.

The data subject has the right to choose the specific scope of the data disclosed under (d), (e) and (h) or not to disclose the data at all.

3) The data referred to in paragraph 2) may only be published on:

a) university employees;

b) University students who are currently serving on the University's self-governing academic or advisory bodies.

4) In the case of persons serving on self-governing academic or advisory bodies of the University who are not in an employment relationship with the University, only the personal data referred to in paragraph 2)(a) and (b) shall be disclosed; any extension of the scope of the disclosed personal data of these persons shall be subject to their prior consent to such disclosure.

Article 11

Disclosure of personal data to third parties

1) Personal data may only be disclosed to third parties in accordance with the rules set out in this Directive and in accordance with the Regulation and applicable generally binding legislation.

2) The disclosure of personal data to third parties may only be made in the context of the activities listed in the register pursuant to Article 9, including the named recipient of the third party for that activity.

3) In other cases, the intention to disclose personal data to a third party must be notified in writing in advance to the Data Protection Officer, stating the scope of the data disclosed, the purpose of the disclosure and the identification of the third party.

4) The person referred to in Article 3(2) shall be responsible for ensuring that the correct procedure for the disclosure of personal data to third parties is followed.

Article 12

Provision of information at the request of the data subject

1) The data subject has the right to request:

a) access, correction or deletion of personal data;

b) processing limitations;

c) data portability;

d) objecting to processing.

2) These requests shall be made by the data subject in the form of a written request or through an authorised representative. In the event that the data subject requests any matter related to the processing of their personal data and the exercise of their rights from a University employee other than the Data Protection Officer, the data subject shall provide the contact details of the Data Protection Officer to the requester and shall notify the Data Protection Officer thereof without delay.

Article 13

Final provisions

1) This Directive shall become valid on the date of its signature.
2) This Directive shall become effective on the date of its publication on the intranet.

In Opava on

doc. Ing. Pavel Tuleja, Ph.D.
Rector

Appendices:

Appendix 1 – Sample of the employee's familiarisation with the principles, rules and procedures for processing personal data

Appendix 2 – Consent to the processing of personal data

Appendix 3 – Notification of new activities / changes in personal data processing activities

University constituent:	Rector's Office
Designation:	**Rector's Directive**
Number:	**10 /2018**
Directive title:	**Personal Data Protection and Processing**
Approved by:	Doc. Ing. Pavel Tuleja, Ph.D.
Valid from:	On the date of publication
Effective from:	On the date of publication
Date of publication:	
Issued by:	Rector
Processed by:	Mgr. Bc. Ondřej Lušňák
In cooperation with:	Ing. Ivana Růžičková, Mgr. Tomáš Gongol, Ph.D.
Number of pages:	11
Number of appendicess:	3
Method of publication	Public area of the website/intranet