ORDER OF THE RECTOR

NO. 04/2018

on the Protection and Processing of Personal Data at Czech Technical University in Prague

Part One

Basic provisions

Article 1

Subject of modification

(1) This order establishes the principles and rules for the processing of personal data within the Czech Technical University in Prague (hereinafter referred to as the "University"), sets out 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) The subject of this order is the processing of personal data by employees and students of the University in the performance of their work or study duties, or by other natural and legal persons who process personal data on the basis of a contract or other relationship with the University.

(3) This order is based, first of all, on

a) 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) /hereinafter referred to as the "Regulation"/,

b) Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendments to Certain Acts, as amended (hereinafter referred to as the "Personal Data Protection Act"),

with the addition and elaboration of some of their provisions for the regulation of relations within the University and provides for organizational solutions within the University to ensure their implementation.

Article 2

Interpretation of selected relevant terms

For the purposes of this Order, the following shall mean:

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 means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction;

3) "controller" means CTU as the entity which alone or jointly with others determines the purposes and means of processing personal data;

4) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data for the controller;

5) "profiling" means any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or estimate aspects relating to the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

6) 'pseudonymization' means the processing of personal data in such a way 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 organizational measures to ensure that it is not attributed to an identified or identifiable natural person;

7) 'register' means any structured set of personal data accessible according to specific criteria, whether centralized, decentralized or disaggregated by function or geography;

8) 'recipient' means the natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether or not it is a third party. Public authorities which may receive personal data in the context of a special investigation in accordance with the law of a Member State shall not be considered as recipients; the processing of such personal data by those public authorities shall comply with the applicable data protection rules for the purposes of the processing;

9) 'third party' means a natural or legal person, public authority, agency or other body which is not the data subject, controller, processor or a person directly under the control of the controller or processor who is authorized to process personal data;

10) "consent" of the data subject means any free, specific, informed and unambiguous expression of the data subject's will by which he or she gives his or her consent to the processing of his or her personal data by means of a declaration or other manifest acknowledgement;

11) "personal data breach" means a breach of security which results in the accidental or unlawful destruction, loss, alteration or unauthorized 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 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 relating to the physical, physiological or behavioural characteristics of a natural person which enables or confirms unique identification, such as facial 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 his or her state of health;

Definitions of other terms used in connection with the data protection regulation are set out in Article 4 of the Regulation or in the text or annexes to this Order where appropriate.

Part Two

Responsibilities of Data Protection Officers

Article 3

Status of the University

The University is the entity responsible for the processing of the personal data referred to in Article 1(2) of this Order. Depending on the specific cases, the University may act as both controller and processor. In order to fulfil the protection of personal data as required by the Regulation and the Data Protection Act, the persons involved in ensuring the above purpose are set out in Part Two of this Order.

Article 4

Central level

(1) The position of the Rector is determined by law[1], the Statutes of the University and other internal regulations and standards of the University. The Rector shall act as the statutory authority of the University responsible for ensuring compliance with the principles, rules and procedures for the processing of personal data externally and internally within the University, in cases implemented at the central level of the University and where there has been no shift of authority to other persons listed in this section.

(2) The Bursar is accountable to the Rector of the University for compliance with the principles, rules and procedures for processing personal data implemented in the areas of his/her competence given by the internal regulations of the University, the relevant competence order of the Rector[2], and other standards of the University.

(3) Vice-Rectors are responsible to the Rector of the University for compliance with the principles, rules and procedures for the processing of personal data carried out within the scope of their activities and competences as defined by the internal regulations of the University, the relevant Rector's competence order[2], and other University standards.

Article 5

Faculties, university institutes and other parts of the University

(1) The deans of the individual faculties of the University are responsible to the Rector for compliance with the principles, rules and procedures for processing personal data by employees and students of the faculty of the University in the performance of their work or study duties, or by other natural and legal persons who process personal data on the basis of a contract with a faculty of the University in matters entrusted to them by the provisions of Section 24 of the Act[1], and by the internal standards of the University[3].

(2) The directors of the University's higher education institutes are responsible to the Rector of the University for compliance with the principles, rules and procedures for the processing of personal data carried out by employees of the University's higher education institute in the performance of their duties, or by other natural and legal persons who process personal data on the basis of a contract with the University's higher education institute in matters entrusted to them by the internal standards of the University.

(3) Persons heading other units of the University (other than those listed in paragraphs 1 and 2) are responsible to the Rector for compliance with the principles, rules and procedures for processing personal data by employees of the University's facilities in the performance of their duties, or by other natural and legal persons who process personal data on the basis of a contract with the University's facilities in matters entrusted to them by the University[4]'s internal standards.

---

[1] Act No. 111/1998 Coll., on higher education institutions.

[2] Rector's Order No. 9/2014 to determine the duties, powers and responsibilities of the Vice-Rectors, the Bursar and the Chancellor of CTU

[3] Rector's Order No.1/2004 on the determination of the powers and duties of the deans of faculties and directors of university institutes of CTU.

[4] Rector's Order No. 2/2004 on the determination of the powers and duties of the directors of other CTU units.

Article 6

Guarantor of personal data processing

(1) In order to ensure the protection of personal data and its processing in accordance with the Regulation and the Personal Data Protection Act, personal data processing guarantors (hereinafter referred to as "PDP Guarantor") are appointed for individual cases or areas of processing.

(2) The PDP Guarantor is the person responsible for compliance with the principles, rules and procedures (set out in this Order and other relevant generally binding legal regulations) for the processing of personal data carried out in the case, or area or responsibility entrusted to him/her. The PDP Guarantor is responsible for ensuring the above requirements from the date of his/her appointment as PDP Guarantor until the termination of the activity, including ensuring the secure archiving of data in accordance with the Regulation.

(3) In the area entrusted to him, the PDP Guarantor shall be responsible for carrying out an impact assessment of the intended processing operations on the protection of personal data pursuant to Article 35 of the Regulation. If he/she assesses that the type of processing chosen by him/her, in particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing, the PDP Guarantor shall carry out a data protection impact assessment of the intended processing operations. For this purpose, he/she shall request the opinion of the Data Protection Officer.

(4) The PDP Guarantors for each case/area are determined by:

a) Rector for the processing of personal data affecting the entire University;
b) dean, director of a higher education institute, director of another unit of the university in the processing of personal data within the scope of the faculty, higher education institute, other unit;
c) the dean, the director of the higher education institute, the director of another unit where the processing involves more than one specific unit. In the event that no PDP Guarantor is appointed, the Rector shall appoint the PDP Guarantor.

(5) In the case of existing areas of processing of personal data, the PDP Guarantor shall be appointed by the persons referred to in Articles 4 and 5 no later than ten days after the entry into force of this Order. In the case of new areas, the PDP Guarantor shall be appointed before the processing of personal data begins.

(6) The persons referred to in paragraph 4 shall immediately inform the Data Protection Officer of the appointment of the PDP Guarantor.

Article 7

Other authorized persons

(1) The following persons may come into contact with personal data:

a) the persons who, according to the characteristics of the relevant data processing according to Article 13, are responsible for entering and disposing of personal data;
b) persons who are superior to the persons referred to in point (a) in terms of organization or methodology;
c) persons who ensure the organizational, functional and technical administration of the relevant data processing (usually analysts, programmers, system and network administrators, departmental clerks, etc.);
d) other persons who, according to the characteristics of the relevant data processing pursuant to Article 13, are authorized to use the personal data for the performance of their tasks.

(2) Other authorized persons are designated by the PDP Guarantor for specific cases/areas. The recruitment or reassignment of persons to posts with the authorization referred to in paragraph 1 shall be subject to their prior demonstrable familiarity with this Order, the Regulation and other relevant generally applicable legislation.

(3) The persons referred to in paragraph 1 are always obliged to process personal data only within the scope of the conditions of implementation/type solution of the respective data processing according to Article 6.

(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 jeopardize the security of personal data. The

obligation of confidentiality shall continue after the termination of the employment, study or work concerned.

Article 8

Final and other student theses

In cases where personal data would be processed for students' final theses (bachelor, master, rigorous and dissertation), the supervisor is obliged to inform the student about the obligations under the regulation and the order and to ensure any further steps in accordance with the order. In general, this obligation also applies in other cases where the student is processing a project or other activity in the course of his/her duties in which personal data are processed.

Part Three

Data Protection Officer

Article 9

Appointment of the Data Protection Officer

The Data Protection Officer at the University (hereinafter referred to as the "Officer") shall be appointed by the Rector on the basis of his/her professional qualities, in particular his/her expertise in law and practice in the field of personal data protection and his/her ability to perform the tasks referred to in Article 11.

Article 10

Position of the Data Protection Officer

(1) The Officer is an employee of the University and reports directly to the Rector.
(2) The Officer is involved in all processes and matters relating to the protection and processing of personal data at the University.
(3) The Officer shall be supported by the University in maintaining his/her expertise and shall be given access to personal data, processing operations and all resources necessary for the performance of the tasks referred to in Article 11.
(4) No specific instructions are given to the Data Protection Officer by the University regarding the performance of his/her duties as a Officer. However, he/she may be assigned other tasks and duties by the Rector. However, none of these tasks or duties shall give rise to a conflict of interest with the performance of the duties of the Officer.
(5) The Officer shall be bound by confidentiality in connection with the performance of his/her tasks. The obligation of confidentiality shall continue after the termination of the employment relationship with the University.
(6) Details of the Officer, including contact details, are provided in the public section of the University's website.

Article 11

Tasks of the Data Protection Officer

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

a) provide information and advice to students and University staff who process personal data on their obligations under this Order, the Regulation and other generally binding data protection legislation;
b) monitor compliance with this Order, the Regulation, other generally binding data protection legislation and the University's data protection policies, including the allocation of responsibilities, awareness raising and training of staff involved in processing operations and related audits;
c) supervises the implementation of the protection and processing of personal data;
d) provide advice and technical assistance upon request as regards the data protection impact assessment and monitor its application pursuant to Article 35 of the Regulation;

e) reporting personal data breaches to the supervisory authority (Article 33 of the Regulation) and notifying personal data breaches to the data subject (Article 34 of the Regulation), after prior consultation with the persons referred to in Articles 4 and 5;
f) cooperates and communicates with the supervisory authority;
g) act as a contact point for the supervisory authority on matters relating to the processing of personal data, including prior consultation pursuant to Article 36 of the Regulation, and, where appropriate, conduct consultations on any other matter;
h) receives proposals from the PDP Guarantors to initiate new or change the existing processing of personal data and takes opinions on such proposals;
i) communicate with data subjects who may contact him/her on any matter relating to the processing of their personal data and the exercise of their rights under this Order and the Regulation;
j) perform other duties arising for his/her position from regulations, law or other generally binding legislation, or arising from this Order and other University regulations.

(2) The Officer shall oversee the operation of the University's data processing registers referred to in Article 13.

(3) In carrying out its tasks, the Officer shall take due account of the risk associated with the processing activities, while taking into the account the nature, scope, context and purposes of the processing.

Article 12

Competences of the Data Protection Officer at the University

(1) If the Officer becomes aware of a breach risk of the rules regarding the protection of personal data arising from the Regulation, the Act or this Order, or if a breach is detected, the Officer must notify the PDP Guarantor and recommend in writing that the defective or risky situation be remedied. The PDP Guarantor shall discuss the situation with the Officer within a reasonable period of time and. If the PDP Guarantor agrees with the Officer's findings, he/she must refrain from further defective or risky conduct. The PDP Guarantor shall also take all measures to prevent a recurrence of the situation. If the PDP Guarantor disagrees with the recommendation of the Officer, he/she shall provide the Officer with a written explanation of the conduct in question and the reasons why he/she considers the rules referred to in the first sentence not being at risk of infringement. In such a case, the Officer shall notify the relevant persons referred to in Articles 4 and 5 and forward the entire file to them.

(2) If there is a risk of a violation of the rules on the protection of personal data arising from the Regulation, the law or this order, or if a violation is detected and a PDP Guarantor has not been appointed for a given case/area/processing activity, the Officer is obliged to notify the relevant persons referred to in Articles 4 and 5 in writing.

(3) The Officer shall be obliged to initiate general or individual data protection measures to the persons referred to in Articles 4 and 5 whenever:

a) on the basis of its findings under paragraph 1, determines that there is a threat of a breach or violation of the rules;
b) it will be appropriate following the development of knowledge and techniques in the field of data protection.

(4) The provisions of paragraphs 1 to 3 shall be without prejudice to the obligation of the Data Protection Officer, after prior consultation with the persons referred to in Articles 4 and 5, to report a personal data breach to the supervisory authority and to the data subject pursuant to Article 11(1)(e).

Part Four

Register of the processing of personal data of the University

Article 13

Registration and recording of personal data processing

(1) In order to provide an overview of the processing of personal data at the University, an electronic register of personal data processing activities at the University (hereinafter referred to as the "Register") is

established. The Computing and Information Centre (hereinafter referred to as the 'VIC') is responsible for the operation of the Register. The Director of the VIC is responsible for the operation of the Register.

(2) University units that process and/or wish to process personal data protected by this Order, or wish to change the current way they process personal data, shall notify the Data Protection Officer.

(3) The notification referred to in paragraph 2 shall contain a full description of the personal data processing concerned. The scope shall be determined by the University's arrangements.

(4) The PDP Guarantor shall always request a prior opinion from the Offficer on the implementation procedure and the setting up of a standard solution for the protection of personal data processed here.

(5) The PDP Guarantor has the right to start new or change the existing processing of personal data only after receiving an official opinion from the Officer on the basis of the result of the notification. If the opinion is negative, the persons referred to in Articles 4 and 5 shall be consulted on the matter.

Part Five

Personal data processing principles

Article 14

Personal data processing principles

(1) The principles for processing personal data are set out in Chapter 2 of the Regulation. Personal data must comply with the Regulation in the following manner:

a) processed in a lawful, fair and transparent manner in relation to the data subject;
b) collected for specific, explicit 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, where necessary, up-to-date; all reasonable measures shall be taken to ensure that personal data which are inaccurate, having 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 organizational measures against unauthorized or unlawful processing and against accidental loss, destruction or damage.

(2) The persons referred to in Part Two of this Order shall be responsible for compliance with the principles set out in paragraph 1 and shall also be able to demonstrate such compliance.

Article 15

Legality of processing

(1) In accordance with Article 6 of the Regulation, processing is lawful only if at least one of these conditions is met and only to the relevant extent:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (The conditions of consent are detailed in Articles 7 and 8 of the Regulation);
b) the processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of measures taken prior to the conclusion of the contract at the request of the data subject;
c) the processing is necessary for compliance with a legal obligation to which the controller is subject, in accordance with applicable generally binding legal provisions;
d) the processing is necessary to protect the vital interests of the data subject or another natural person;
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, in accordance with applicable generally binding legal provisions;

f) the processing is necessary for the purposes of the legitimate interests of the controller or third party concerned, 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.

(2) Paragraph 1(f) shall not apply to the processing of personal data by the University in cases where the University acts as a public authority in matters entrusted to it by law.

(3) 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, the PDP Guarantor shall take into account, inter alia, the following in order to determine whether the processing for the other purpose is compatible with the purposes for which the personal data were originally collected:

a) any 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 special categories of personal data are processed pursuant to Article 9 of the Regulation or personal data relating to criminal convictions and offences pursuant to Article 10 of the Regulation;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymization.

Article 16

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 shall be prohibited in cases not covered by paragraphs 2 and 3.

(2) The exceptions to the prohibition of processing of personal data under paragraph 1 are provided for in Article 9 of the Regulation.

(3) Exceptions to the prohibition in paragraph 1 include data on:

a) health status in the personal records of employees and students, provided that such data have been voluntarily provided by the data subject to the mentioned records and are kept for his/her benefit (e.g. they affect admission to studies, the provision of services to persons with specific requirements, accommodation in dormitories or the calculation of his/her tax liability or other statutory benefits);

b) membership of trade unions operating at the University as recorded in the personal and payroll records of employees, provided that they have been voluntarily submitted by the data subject to the mentioned records and are used for the payment of membership fees or other benefits, including accounting for such payments;

c) biometric data which allow direct identification or authentication of the data subject, provided that sufficient technical and organizational measures are taken;

d) special categories of personal data processed for project/research purposes.

(4) 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 what data it relates to, for what purpose, for what period and by whom. By signing it, the data subject also confirms that he or she has been informed of his or her rights in advance. Authorized persons who, according to the characteristics of the relevant data processing according to Article 6, are intended to

enter and dispose of the data referred to above, shall be able to prove the existence of such consent throughout the processing.

(5) The processing of personal data that does not require the identification of the data subject is governed by Article 11 of the Regulation.

Part Six

Data subject

Article 17

Information provided to the data subject

(1) The University, in its role as controller, shall provide the data subject with all the information referred to in Articles 13 and 14 of the Regulation in a concise, transparent, comprehensible and easily accessible manner using clear and plain language, in accordance with Article 12 of the Regulation, and shall make all the disclosures referred to in Articles 15 to 22 and 34 of the Processing Regulation. The information shall be provided in electronic form on the University's website and in the University's information systems.

(2) Data subjects may contact the Data Protection Officer in all matters relating to the processing of their personal data and the exercise of their rights under this Order and the Regulation.

Article 18

Rights of the data subject

The right of the data subject to:

a) access to personal data is governed by Article 15 of the Regulation;
b) the correction is governed by Articles 16 and 19 of the Regulation;
c) the deletion is governed by Articles 17 and 19 of the Regulation;
d) The processing restrictions are governed by Articles 18 and 19 of the Regulation;
e) Data portability is regulated by Article 20 of the Regulation;
f) objection and automated individual decision-making are governed by Articles 21 and 22 of the Regulation.

The specific manner of implementation of these data subject rights is the responsibility of the PDP Guarantor.

Part Seven

Disclosure and security of personal data and disclosure to third parties

Article 19

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 protected under this Order may be disclosed to the extent of:

a) name;
b) last name;
c) titles;
d) photographs;
e) job assignment at the university;

f) inclusion in the organizational structure of the University;
g) positions held at the university;
h) contact details in connection with the University (addresses of departments, telephone and fax numbers, e-mail addresses);
i) biography;
j) the course of academic qualification;
k) participation in the various forms of creative activity of the University;
l) information on publications;
m) teaching carried out at the university;
n) academic personal websites (i.e. websites of university employees and students related to their academic or study activities at the university),
o) other data that the subject has published here about himself/herself.

The data referred to in points (d), (i), and (n) may be disclosed only with the prior consent of the data subject to the extent and under the conditions specified by the data subject.

(3) The data referred to in paragraph 2 may only be disclosed on data subjects who:

a) are employees of the University; or
b) are employees or students of the University and currently serve on self-governing academic or advisory bodies of the University.

(4) In the case of academic officials and heads of units of the University, the disclosure of personal data will be regulated individually.

(5) In the case of academic officials and persons currently serving on self-governing academic or advisory bodies of the University who are not in an employment relationship with the University, the disclosure of personal data will be regulated individually.

Article 20

Disclosure of personal data to third parties

(1) The disclosure of personal data to third parties outside the University is governed by this Order, the Regulation and applicable generally binding legal regulations and other internal standards of the University.

(2) Any disclosure of personal data to a third party outside the University 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.

(3) It is the responsibility of the PDP Guarantor appointed for the specific case/area of processing to ensure that the correct procedure is followed for the provision of personal data to third parties outside the University in accordance with this Order, the Regulation and applicable generally binding legal provisions. If there is no PDP Guarantor appointed for the case/processing area, the persons referred to in Articles 4 and 5 shall be responsible for compliance with the correct procedure for the disclosure of personal data to third parties outside the University.

Article 21

Security of personal data

(1) The methods of ensuring the security of information, including personal data, are described below:

a) in other internal standards governing the rules of safe user behaviour[5],

[5] Guidelines for safe user behaviour.

b) in the Overview of Minimal Security Requirements for Suppliers[6].

Part Eight

Final provisions

Article 22

Final provisions

(1) Rector's Order No. 5/2015 on the protection of personal data at CTU is hereby repealed.

(2) Compliance with this order shall be monitored by the appointed Data Protection Officer; all units shall provide the Officer with the necessary cooperation to carry out this monitoring.

(3) This Order shall take effect on 23 May 2018.

doc. RNDr. Vojtěch Petráček, CSc., v. r.
Rector

[6] Annex 4 of the Personal Data Processing Agreement