

Code:	SR/9/2018
Category:	RECTOR'S DIRECTIVE
Title:	Protection and Processing of Personal Data
Liability:	Tomas Bata University in Zlín
Issue date:	30 April 2018
Effective:	1 May 2018
Issued by:	Prof. Ing. Petr Sáha, CSc., Rector
Prepared by:	Legal Services
In cooperation with:	Data protection officer
Pages:	13
Appendices:	4
Distribution list:	TBU Employees and Students
Signature of authorized person:	Prof. Ing. Petr Sáha, CSc., m.p.

PART ONE
Basic Provisions

Article 1
Scope of Application

- (1) This Directive shall specify the principles and rules for the processing of personal data within Tomas Bata University in Zlín (hereinafter referred to as "TBU" or "University"), liabilities of persons in charge of the protection of personal data at TBU, define rights and responsibilities of employees, students or other natural or legal persons participating in activities related to the processing of such data.
- (2) The scope of application of this Directive is processing of personal data carried out by employees upon performance of their professional duties, or by other natural or legal persons processing personal data in compliance with a contract concluded with TBU.
- (3) This Directive is based on the 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 free movement of such data and on repeal of Directive 95/46/ES (general data protection regulation, hereinafter referred to as "GR") and on the Act No. 101/2000 Coll., on the Protection of Personal Data and on Alterations to Some Acts, as amended (hereinafter referred to as the "Act"), and amends and elaborates on some of their provisions for the arrangement of relations within TBU and shall set an organizational system within TBU ensuring their implementation.

Article 2
Definition of Selected Terms

- (1) *Personal data* means any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject"). An identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to a certain identifier, for example, name, identification number, location data, network identifier or to one or more factors specific to the physical, physiological, genetic, psychical, economic, cultural or social identity of the natural person (hereinafter also referred to as "PD").
- (2) *Processing of personal data* means any operation or set of operations which is performed on 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 otherwise making available, alignment or combination, restriction, erasure or destruction.

- (3) *Controller* means the natural or legal person, public authority, agency or other subject which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by the European Union law (hereinafter referred to as the “Union”) or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- (4) *Processor* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- (5) *Profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- (6) *Pseudonymisation* means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- (7) *Filing system* means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- (8) *Recipient* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union Member State law shall not be regarded as recipients; the processing of those personal data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- (9) *Third party* means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
- (10) *Consent of the data subject* means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- (11) *Personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (hereinafter referred to as “incident”).
- (12) *Genetic data* means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- (13) *Biometric data* means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, for example, facial images or dactyloscopic data.
- (14) *Data concerning health* means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
- (15) Definitions of other terms used for dealing with and protection of personal data are specified under Article 4 of the general regulation, or in the text of this Directive or in the Appendices

thereof, where it is efficient.

PART TWO

Liability of Persons in Charge of Protection of Personal Data

Article 3

Status of the University

TBU is a subject responsible for the processing of personal data specified under Article 1 Paragraph 2 of the Directive. Depending on particular cases, the University may perform the role of controller, as well as the role of processor of personal data. In order to comply with the protection of personal data as is required by the general regulation and the Act, TBU employees participating in the fulfilment of the abovementioned purpose are specified in Part Two of this Directive.

Article 4

Liability at the Level of Faculty and Other Component Parts

- (1) The status of the Rector is defined by the Act, Statute of the University and other internal regulations of the University. The Rector acts as a statutory body of the University liable for the observance of principles, rules and procedures for the processing of personal data in and outside the University, and that in cases carried out at the centralized level of the University and in cases in which no transfer of powers to other persons specified in this Part took place.
- (2) The Bursar shall be liable to the Rector of the University for the observance of principles, rules and procedures for the processing of personal data carried out within the scope of his/her competence in accordance with Article 22 of the TBU Statute.
- (3) Vice-Rectors shall be liable to the Rector of the University for the observance of principles, rules and procedures for the processing of personal data carried out within the scope of their activity and competence defined by the relevant TBU internal regulations, mainly by relevant legal proceedings taken by the Rector and the Organizational Regulations of TBU Rectorate.
- (4) Deans of relevant Faculties of the University shall be liable to the Rector for the observance of principles, rules and procedures for the processing of personal data carried out by employees of a given Faculty upon performance of their professional duties, or by other natural or legal persons processing personal data in compliance with a contract concluded with the Faculty in matters conferred on them by the TBU Statute, other TBU regulations and rules.
- (5) Head of a TBU department shall be liable to the Rector for the observance of principles, rules and procedures for the processing of personal data carried out by employees of the TBU department upon performance of their professional duties, or by other natural or legal persons processing personal data in compliance with a contract concluded with the relevant University department in matters conferred on them by the TBU Statute, TBU internal regulations and rules.
- (6) Directors of other TBU component parts shall be liable to the TBU Rector for the observance of principles, rules and procedures for the processing of personal data carried out by employees of the relevant TBU component part upon performance of their professional duties, or by other natural or legal persons processing personal data in compliance with a contract concluded with these TBU component parts in matters conferred on them by the TBU Statute, Organizational Regulations of the relevant component part and other TBU regulations and rules.

Article 5

Coordinator of Personal Data Processing

- (1) The coordinator is liable for the coordination of procedures and outputs according to the general regulation.
- (2) The person appointed as a coordinator of personal data processing is the secretary at Faculties, and usually the financial manager of the component part at relevant component parts. This position shall not be appointed at the Rectorate.
- (3) In the event that a coordinator has not been appointed according to Article 2, it is the person specified in Article 4 of the Directive who shall have the competence of the coordinator, and s/he is obliged to inform the data protection officer (hereinafter referred to as “officer”) about this fact in writing, and that without undue delay.

Article 6

Guarantor of Personal Data Processing

- (1) In order to ensure the protection of personal data and their processing in accordance with the general regulation and with the Act, guarantors of personal data processing (hereinafter referred to as “guarantor”) shall be appointed for particular cases or spheres of processing.
- (2) The guarantor is a person liable for the observance of principles, rules and procedures specified in the general regulation, the Act, this Directive, and other relevant generally binding legal regulations during the processing of personal data carried out within the case/sphere/activity s/he is in charge of. The guarantor is liable for the abovementioned activities from the date of his/her appointment to the date of termination of the activity, and that including ensuring of safe archiving of the data.
- (3) The guarantor provides active and timely assistance in dealing with the request submitted by the data subject.
- (4) The guarantor is also obliged to provide all necessary assistance to all the persons in charge of or otherwise participating in personal data protection.
- (5) The guarantors for particular cases/spheres/activities are:
 - a) at Faculties – secretary, head of student affairs office, head of the relevant Vice-Dean’s office or offices subordinate to the Dean. If such a senior executive has not been appointed, the coordinator of personal data processing shall become the guarantor;
 - b) at component parts - head of the relevant office; if such a senior executive has not been appointed, the coordinator of personal data processing shall become the guarantor;
 - c) at the Rectorate – head of the particular divisions and offices, in case of an office subordinate to Vice-Rector it is the Vice-Rector who shall have the competence of the guarantor, in case of the Rector’s Office it is the Rector who shall have the competence of the guarantor, and in case of the Bursar’s Office it is the Bursar who shall have the competence of the guarantor.
- (6) In the event that personal data processing systems have already been in operation, the guarantor shall be appointed on the day on which this Directive becomes effective. In the event that new systems have been launched, the guarantor shall be specified prior to the initiation of data processing.
- (7) Persons specified in Article 4 of the Directive shall inform the data protection officer about the appointment of a new guarantor in writing without delay.

Article 7

Other Authorized Persons

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

- a) persons that are according to the specification of the relevant data processing in compliance with Article 13 authorized to include and discard personal data;
 - b) persons that are superior to the persons listed in Letter a) in terms of organizational or methodological scheme;
 - c) persons who ensure organizational, functional and technical management of the relevant data processing (usually analytics, programmers, administrators of systems and networks, officers at relevant offices, etc.);
 - d) other persons that are according to the specification of the relevant data processing in compliance with Article 13 authorized to use these personal data to fulfil their tasks.
- (2) Other authorized persons shall be appointed by the guarantor. Admission or transfer of persons to the positions of authorized persons in accordance with Paragraph 1 is conditional upon the fact that they have been conclusively acquainted with this Directive, with the general regulation and other relevant generally binding legal regulations.
- (3) Persons specified in Paragraph 1 are obliged to process personal data only to the extent required by the implementation/dealing with a specific type of relevant data processing in accordance with Article 6.
- (4) Persons specified in Paragraph 1 are obliged to maintain secrecy concerning personal data and concerning security measures, whose publication would threaten security of personal data. The obligation to maintain secrecy shall be observed even after termination of employment relationship or after relevant work has been completed.

Article 8

Theses and Other Student Projects

- (1) In the event that personal data are processed in student theses (Bachelor's, Master's, advanced Master's or doctoral theses), the supervisor is obliged to acquaint students with obligations in accordance with the general regulation and this Directive and take further steps in compliance with the Directive, if need be.
- (2) The obligation specified in Paragraph 1 applies also to those cases in which students carry out activities within which personal data are processed, either during the fulfilment of their academic requirements or not.

PART THREE

Data Protection Officer

Article 9

Appointment of the Data Protection Officer

The data protection officer shall be appointed by the Rector on the basis of his/her professional qualities and, in particular, expert knowledge of and experience in the sphere of personal data protection and the ability to fulfil the tasks specified in Article 11.

Article 10

Establishment of Position and Staffing

- (1) The data protection officer is an employee of the University, included in the organizational chart of the TBU Rectorate and s/he is directly subordinate to the Rector.
- (2) The position of the data protection officer shall be established in compliance with the general regulation as an obligation of a public authority that TBU has.
- (3) In the event that the data protection officer is absent, a TBU Legal Services lawyer (hereinafter referred to as "deputy data protection officer") shall act as his/her deputy. In such a case the data protection officer shall provide assistance necessary for the tasks of the data

protection officer to be fulfilled by the deputy data protection officer.

- (4) The deputy data protection officer is directly subordinate to the TBU Rector for the period of the performance of duties of the data protection officer.
- (5) Information about the data protection officer including contact details shall be mentioned on a publicly accessible part of the TBU website.

Article 11

Scope of Activities and Competence of the Data Protection Officer

- (1) The data protection officer shall perform the following tasks set in the General Regulations:
 - a) Continuously monitor the policy followed at TBU during the processing of personal data in the context of compliance with the General Regulations, other regulations of the Union or of the Union Member States in the area of personal data protection; at the same time, all component parts of TBU are obliged to offer any collaboration necessary.
 - b) Carry out consultation and counselling activities relating to the sphere of personal data at TBU and aimed at creating a policy in compliance with the General Regulations and, at the same time, intended for data subjects (in particular employees and students), who may contact the data protection officer in all matters relating to the protection of their personal data.
 - c) Supervise the implementation of personal data protection and processing.
 - d) Provide consultations during cases of a personal data breach, assess the gravity of the respective case of a personal data breach.
 - e) Issue recommendations relating to the notification of the supervisory authority/data subject, when applicable, and propose appropriate measures.
 - f) After prior consultations with persons listed in Article 4, ensure notification of cases of a personal data breach to the Office for Personal Data Protection (hereinafter referred to as “supervisory authority”) and notification of cases of a personal data breach to the data subject.
 - g) Accept proposals from employees of the University regarding the commencement of a new procedure, or regarding the modification of the procedure previously used for the processing of personal data and gives his/her opinions thereto.
 - h) Communicate with data subjects, who may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights in compliance with the General Regulations and with this Directive.
 - i) Cooperate with the supervisory authority.
 - j) Act as the contact point for the supervisory authority in issues relating to personal data processing and as the central place for the notification of incidents.
 - k) Regularly inform the Rector on issues relating to the performance of tasks connected with the position of the data protection officer. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks. The obligations of secrecy also apply after the performance of the position of the data protection officer has ended.
- (2) The data protection officer is involved in all procedures and issues which relate to the protection and processing of personal data at TBU and attends all meetings dealing with the personal data processing.
- (3) The data protection officer shall supervise the functioning of the Register of Processing of Personal Data of the University as specified in Article 13.
- (4) The data protection officer shall be supported by TBU in maintaining his or her expert knowledge and provided access to personal data, processing operations and all sources necessary to carry out these tasks.
- (5) If the data protection officer is notified about an existing danger of a breach of rules for personal data protection set in the General Regulations, the Act or this Directive, or if such a

breach has been detected, he/she is obliged to notify such a case to the guarantor and recommend the remedy of the harmful or hazardous situation in writing. The guarantor is obliged to remedy the harmful or hazardous situation without undue delay. In the event that the guarantor fails to remedy such a situation, the data protection officer shall submit the recommendation as to the remedy of the harmful or hazardous situation to persons listed in Article 4, who are obliged to ensure a remedy of such a situation without delay. If those persons do not agree with the recommendations proposed, they are obliged to inform the data protection officer about this fact without undue delay. In such a case, the data protection officer shall inform the Rector, who is, as the statutory body of the University, the person entitled to take a final decision on the remedy of a harmful or hazardous situation.

- (6) If the danger of a personal data breach exists in accordance with the General Regulations, Act, or this Directive, or if such a breach has been detected already and, at the same time, no guarantor has been appointed for the given case/area/activity, the data protection officer is obliged to notify this fact in writing to the persons which have subject-matter jurisdiction and are listed in Article 4.
- (7) In compliance with Article 11 Paragraph 1, Letter d), the provisions of Paragraphs 5 and 6 do not affect the data protection officer's duty to notify a personal data breach to the supervisory authority and to the data subject after prior consultation with persons listed in Article 4.

Article 12

Conflict of Interests

- (1) If the data protection officer finds out that his/her tasks and duties result in a conflict of interests, he/she shall notify this fact to the Rector of TBU.
- (2) The data protection officer's tasks and duties result in a conflict of interests in particular if he/she is permitted to determine the purposes and means of personal data processing.
- (3) The Rector of TBU shall decide as to whether or not there is a conflict of interests. If so, the Rector shall prevent such a conflict by adopting an appropriate organizational measure, e.g. transfer of competence in the given matter to the deputy data protection officer.

PART FOUR

Register of Processing of Personal Data at TBU

Article 13

Registration and Filing of Processing of Personal Data

- (1) In order to obtain an overview on the processing of personal data, the Register of Processing Activities Relating to Data Protection shall be established at TBU (hereinafter referred to as "Register").
- (2) Faculties or TBU component parts which process personal data or want to modify the processing procedure previously used, shall notify the data protection officer about this intent in writing.
- (3) Such notification must, in compliance with Paragraph 2, contain a comprehensive description of the relevant personal data processing. The extent is determined in the Appendix 1 "Categorization of the Areas of Processing of Personal Data at TBU" and Appendix 2 "TEMPLATE Minimum Record on the Personal Data Processing Activity".
- (4) The guarantor shall always request the data protection's officer prior opinion regarding the procedure of the implementation and specification of the dealing with a specific type of protection of personal data to be processed.
- (5) The proposing guarantor is entitled to start a new procedure or make alterations to the

previously used procedures of personal data processing only after receiving an official opinion from the data protection officer based on the result of the notification. If the opinion is negative and the guarantor insists that the alteration proposed is to be made, the procedure to be followed adheres similarly to Article 11 Paragraph 5.

PART FIVE

Principles Relating to Processing of Personal Data

Article 14

Principles Relating to Processing of Personal Data

- (1) Principles relating to processing of personal data are given in Chapter II of the General Regulations. In compliance with the said principles, the personal data must be:
 - a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
 - f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
 - g) Persons listed in Part Two of this Directive are liable for the observance of the principles given in this Article and must also be able to evidence the said observance of the accordance;
 - h) Each TBU employee is liable for carrying out the processing of personal data in compliance with legal regulations of the EU, CR and TBU internal regulations. At the same time, all employees of TBU are obliged to observe these principles.

Article 15

Lawfulness of Processing

- (1) In compliance with the Article 6 of the General Regulations, processing shall only be lawful if at least one of the following conditions applies and solely to the corresponding extent:
 - a) processing is, in accordance with valid generally binding legal regulations, necessary for compliance with a legal obligation to which the controller is subject;
 - b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - c) processing is, in accordance with valid generally binding legal regulations, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - d) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of

personal data, in particular where the data subject is a child.

- e) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Formalities of the expression of the consent are given in Article 7 and 8 of the General Regulations..
- (2) If TBU performs the role of a public authority in matters entrusted to the institution by the law, the processing of personal data carried out by TBU does not concern cases mentioned in Paragraph 1 Letter d).
- (3) Where the processing for a purpose other than that for which the personal data have been collected is not based on valid generally binding legal regulations or on the data subject's consent, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
 - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
 - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
 - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 of the General Regulations, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 of the General Regulations;
 - (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 16

Processing of Special Categories of Personal Data

- (1) 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, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited in cases where the Paragraph 2 and 3 do not apply.
- (2) Exemptions from the ban on processing on personal data in accordance with Paragraph 1 are given in Article 9 of the General Regulations.
- (3) Exemptions from the ban on processing on personal data in accordance with Paragraph 1 include also the following data:
 - a) Data on health status included in personnel files of employees and students provided that such data have been voluntarily submitted to the above-mentioned filing systems by the data subject and are kept to his/her benefit (e.g. may have an impact on the admission to study, provision of services to special needs persons, accommodation in accommodation facilities owned by the University or the calculation of his/her tax liability and other statutory pays);
 - b) Data on membership in trade union bodies established at TBU, included in personnel and salary files of employees provided that such data have been voluntarily submitted to the above-mentioned filing systems by the data subject and are used for payments of membership fees or other pays, including accounting information on such payments;
 - c) Biometric data which enable direct identification or authentication of the data subject.
- (4) Special categories of personal data may be processed for project/research purposes. The processing of data specified in Paragraph 1 may be solely carried out provided that the data subject has given explicit consent to the processing. Such consent must be given in writing, signed by the data subject and must give evidence about what type of data it refers to, for what purpose and period, who gives the consent. By signing the consent, the data subject also

confirms that he/she has been informed about his/her rights prior to signing the consent. Authorized persons who are, according to the specification of the relevant type of data processing as specified in Article 6, entrusted with inclusion and destruction of the mentioned data, are obliged to be able to evidence the existence of such consent during the entire period of the processing thereof.

- (5) Processing of data in compliance with Paragraph 3 Letter c) may be used solely if there is a parallel option of how to achieve the given purpose by using other means of identification or authentication not depending on the biometric data, and the data subject will have a choice between the two of them.
- (6) Processing of personal data which does not require identification of the data subject adheres to Article 11 of the General Regulations.

PART SIX Data Subject

Article 17 Information Provided to the Data Subject

- (1) In compliance with Article 12 of the General Regulations, TBU as the controller shall provide any information specified in Articles 13 and 14 of the General Regulations and any communication under Articles 15 to 22 and 34 of the General Regulations relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in electronic form on the TBU website in the TBU information systems.
- (2) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation. At the same time, the data protection officer is the central place for the submission and filing of requests for the assertion of rights of the data subject. The model scheme for requesting and gaining the right to obtain information is included in Appendix 4.

Article 18 Rights of the Data Subject

- (1) The data subject shall have the right to:
 - a) Access to personal data as specified in Article 15 of the General Regulations,
 - b) Rectification of data as specified in Article 16 to 19 of the General Regulations,
 - c) Erasure of data as specified in Article 17 to 19 of the General Regulations,
 - d) Restriction of processing of data as specified in Article 18 a 19 of the General Regulations,
 - e) Data portability as specified in Article 20 of the General Regulations,
 - f) Object and to automated individual decision-making as specified in Article 21 and 22 of the General Regulations.
- (2) Information concerning the right of data subjects in relation to personal data are also posted on the TBU website.

PART SEVEN

Publication and Protection of Personal Data and Provision Thereof to Third Parties

Article 19

Publication of Personal Data

- (1) The publication of personal data refers to the access provision thereto for individually unspecified persons or groups of persons, in particular through mass media, via another type of public communication or as a part of a public list (e.g. posted in the public part of the TBU website).
- (2) Personal data are permitted to be made public in compliance with Paragraph 1 solely in case of data subjects who are employees or students of the University and are currently members of self-governing academic or advisory bodies of the University or have given their consent to the publication.

Article 20

Provision of Personal Data to Third Parties

- (1) The provision of personal data to third parties outside TBU adheres to the General Regulations, to valid generally binding legal regulations and to this Directive.
- (2) The data protection officer has to be informed in writing in advance about each and every provision of personal data to a third party outside TBU, including information on the extent of the data provided, purpose of the provision and identification of the third party.
- (3) The guarantor appointed to deal with the given case/sphere/activity of processing is liable for the observance of correct procedures to be used during the provision of personal data to third parties outside TBU in compliance with the General Regulations, valid generally binding legal regulations and this Directive. In the event that no guarantor has been appointed for the given case/sphere/activity of processing, persons listed in Article 4, which have subject-matter jurisdiction, are liable for the observance of correct procedures to be used during the provision of personal data to third parties outside TBU.

Article 21

Personal Data Protection

- (1) Documents in writing and mobile/external/portable information storage mediums owned by TBU and containing personal data, must be stored solely in lockable rooms, or, if appropriate, in lockable cabinets in the TBU constituent parts, or in other secure places specified by the characteristic features of the relevant data protection or secured by encryption.
- (2) It is not permitted to leave personal data freely available and unattended.
- (3) In the event that personal data are processed which are closely related to activities carried out at TBU (e.g. attendance records, texts, notepads, attendance list, etc.), the procedure used during the provision of protection shall be represented by a common method so that the risk of misuse of personal data can be prevented. Other obligations stipulated in this Article shall apply to the processing of such personal data only in the extent corresponding to their nature and circumstances of their usual processing.
- (4) Computers and other technical equipment used to store information containing personal data to be protected in compliance with this Directive, must be protected against unauthorized access by unauthorized persons, usually by using privacy passwords, encryption or locking.
- (5) Copies of personal data protected in compliance with this Directive must be made using information storage mediums and stored in lockable cabinets in the TBU constituent parts, or, if appropriate, in other secure places specified by the characteristic features of the relevant

data protection or secured by encryption. In principle, such data must be stored always in another room than the original data.

- (6) Information security used for storage/transfer of personal data which are no longer needed or their service life has ended, must be safely discarded, and a record on the process of discarding thereof shall be kept by the ITC or by the relevant IT departments of TBU component parts.
- (7) In the event that a TBU employee detects or conceives a suspicion that a personal data breach may occur or has occurred, he/she is obliged to inform the data protection officer and persons listed in Article 4 without delay.
- (8) The notification of cases of a personal data breach to the supervisory authority (Article 33 of the General Regulations) and notification of cases of a personal data breach to the data subject (Article 34 of the General Regulations) shall be made by the data protection officer after previous consultation with persons listed in Article 4.
- (9) Technical measures aimed at provision of security of personal data in electronic form:
 - a) Access to personal data is granted solely in the extent necessary for the performance of activities connected with the relevant job position;
 - b) Records shall be kept on the individual roles concerning the IT security, for each of them, the responsibility and the job description has been unambiguously defined in order to reduce the risks arising from the human factor;
 - c) If the IT operation, accounting operations or other externally processed administrative systems require access provision to suppliers, then this access must be provided in compliance with the relevant contract concluded, in accordance with the security documents in such a manner that the personal data security is ensured in- and outside the institution;
 - d) It is permitted to run solely approved, legally acquired and registered SW and HW in compliance with the licence agreement concluded with the producer and the type of use. This SW and HW property is registered and the purchase thereof adheres to the relevant internal regulations of TBU;
 - e) The selection of potential personal data processors for TBU is conditional upon the ability to conclude a processing contract and observe the obligations set in the contract, sufficient personal data security, a good reputation of the supplier in relation to personal data protection, the relevant certification issued by the Office for Personal Data Protection or data protection in general, also, if appropriate, other relevant factors related to the particular purpose of processing;
 - f) Personal and sensitive data are not permitted to leave the protected IT environment of TBU. A remote-access VPN is only enabled when using computers with an encrypted disk and owned by TBU;
 - g) Employees and students are obliged to use for professional or study-related purposes the officially assigned general or personal e-mail addresses finishing with “@utb.cz”;
 - h) The use of public data storages, services and tools (Dropbox, Google Drive, uloz.to, uschovna.cz, torrents, P2P, Basecamp, Slack, etc.) without a contract previously concluded between the service provider and TBU is not permitted.

PART EIGHT
Final Provisions

Article 22
Final Provisions

- (1) This Directive abrogates the Rector's Directive No. 1/2001 – Personal Data Protection in the TBU Information System.
- (2) The Legal Services department of the TBU Rectorate has been entrusted with the interpretation of individual provisions of this Directive.
- (3) The data protection officer shall monitor the observance of this Directive.
- (4) Each senior executive entitled to receive an extra payment for management is obliged to demonstrably acquaint his/her subordinates with this Directive, unless they have been demonstrably instructed by any of the persons listed in Article 4.
- (5) List of appendices:
 - Appendix 1 Categorization of the Areas of Processing of Personal Data at TBU
 - Appendix 2 TEMPLATE Minimum Record on the Personal Data Processing Activity
 - Appendix 3 TEMPLATE Content of the Notification of Cases of Personal Data Breach
 - Appendix 4 Model Scheme for Requesting and Gaining the Right to Obtain Information