COLLECTION OF DECISIONS AND ORDINANCES OF THE UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

Number: R 375 Date: 17 May 2018

Ordinance of the Rector
stipulating the rules for protection and personal data processing

In accordance with Section 10 (1) of Act no. 111/1998 Coll., On Higher Education Institutions and on Amendments and Supplements to some other Acts (Higher Education Act), as amended (hereinafter referred to as Act), and Article 14 of the Statutes of the University of South Bohemia in České Budějovice (hereinafter referred to as University), I issue the following Ordinance:

Part One
Basic Provisions

Article I
Subject of the Ordinance

1. This Ordinance sets out the principles and rules for personal data processing within the university. It stipulates the responsibility of persons providing personal data protection at the university, defining the rights and obligations of employees, students and, where applicable, other natural and legal persons participating in the processing of such data.

2. This Ordinance deals with the personal data processing carried out by employees and students of the university when performing their work or study duties, or by other natural and legal persons who process personal data under a contract agreed with the university.

3. This Ordinance is based on Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to personal data processing and on the free movement of such data and repealing Ordinance 95/46/EC (General Data Protection Regulation) (hereinafter Regulation), and on Act no. 101/2000 Coll., On the personal data protection and on Amendments to Certain Acts, as amended (hereinafter Personal Data Protection Act), with the addition and elaboration of some of their provisions in order to regulate the relations within the university and set relevant organizational solutions.

Article II
Definitions of Selected Terms

1. For the purposes of this Ordinance the following applies:

a) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

b) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

c) ‘controller’ means the natural or legal person, public authority, agency or other body 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

d) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

e) ‘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;

f) ‘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;

g) ‘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;

h) ‘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 or Member State law shall not be regarded as recipients; the processing of those data by those

public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

i) '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 authorised to process personal data;

j) '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;

k) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

l) '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;

m) '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, such as facial images or dactyloscopic data;

n) '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;

2. Definitions of other terms used in the processing and personal data protection are provided in Article 4 of the Regulation or in the text or annexes of this Ordinance where appropriate.

Part Two
Responsibility and Liability of Persons Ensuring Data Protection

Article III
University Status

The University is the entity responsible for the personal data processing referred to in Art. I (2) of this Ordinance. According to the circumstances of the particular case, the university may act both as a controller and as a processor. The second part of this Ordinance specifies the persons involved in the personal data protection as required by the Regulation and the Personal Data Protection Act.

Article IV
Central Level

1. The Rector's position is determined by law, university Statutes and other internal regulations of the university. The Rector acts as the statutory body of the university responsible for compliance with the principles, rules and procedures of personal data processing both inside and outside the university in cases conducted at the university's central level and where there has been no shift of competence to other persons listed in this section.

2. The Bursar is responsible to the university Rector for observing the principles, rules and procedures for the personal data processing carried out within their competence and activities pursuant to Article 3 (3) and Annexe no.2 of the Organizational Rules of the university Rectorate.

3. The Vice-Rectors are responsible to the university Rector for observing the principles, rules and procedures for processing personal data carried out within their competence and activities pursuant to Article 3 (2) and Annexe no. 2 of the Organizational Rules of the university Rectorate.

Article V
Heads of Individual Constitutional Parts

1. Deans of individual faculties of the university are responsible to the Rector for adherence to principles, rules and procedures in the personal data processing carried out by employees and students of the respective faculty during performance of their work or study duties, or by other natural and legal persons who process personal data on the basis of a contract concluded with the faculty in matters entrusted to it by Section 24 of the Act; Art. 15 of the university Statutes and other internal regulations and university regulations.

2. Directors of other units focusing on teaching and creative activities or for the provision of information services within the meaning of Article 12 (3). of the university Statutes (hereinafter referred to as the university unit), are responsible to the university Rector for observing the principles, rules and procedures for processing personal data carried out by employees of the given university unit in the performance of their duties, or other natural and legal persons who process personal data under the contract with the university unit in matters entrusted to it by the internal regulations of the university or the given university unit.

3. Directors of specialized units for cultural and sports activities, accommodation and catering or for operational units of the university within the meaning of Article 12 (4).of the University Statutes (hereinafter referred to as specialized units) are responsible to the university Rector for compliance with the principles, rules and procedures for processing personal data carried out by employees of the specialised unit in the performance of their duties, or other natural and legal persons who process personal data under the contract concluded with the specialised unit in matters entrusted to it by the internal regulations of the university or the specialised unit.

Article VI
Guarantor of Personal Data Processing

1. In order to ensure the personal data protection and their processing in accordance with the Regulation and the Personal Data Protection Act, personal data processing Guarantors (hereinafter Guarantor) are designated for individual processing or its areas (i.e. several similar processes).

2. Guarantor is a person responsible for adhering to the principles, rules and procedures (stipulated in this Ordinance, the Regulation and other relevant generally binding legislation) during personal data processing performed in the area entrusted to them. The Guarantor is responsible for the listed activities from the date of their appointment to the end of their activity, including ensuring secure data archiving.

3. The Guarantor carries out in their processing/assessment of the impact of any intended processing operations on the personal data protection under Article 35 of the Regulation. For this purpose, they will request the opinion of the data protection Officer.

4. The Rector will appoint Guarantors with a whole-university competence for individual processing/areas under Part A of the university Personal Data Processing Register (see Art. XIII (2) of this Ordinance).

5. Heads of the constituent parts of the university will appoint Guarantors with a limited area of responsibility for individual processing/areas under Part B of the university Personal Data Processing Register (see Art. XIII (2) of this Ordinance).

6. In situation where personal data is already being processed, the Guarantor will be appointed within ten days after the effective date of this Ordinance. For newly introduced processing, the Guarantor will be appointed before the personal data processing commences.

7. The persons referred to in paragraphs 4 and 5 of this Article immediately inform the data protection Officer of the appointment of the Guarantor.

Article VII
Other Authorized Persons

1. There are other authorized persons who may come into contact with personal data:

   a) persons who, depending on the nature of the relevant data processing under Article XIII entrusted with the input and disposal of personal data;

   b) persons who are superior to those referred to in letter a) under organizational or methodological line;

   c) persons who provide organizational, functional and technical management of the relevant data processing (usually analysts, programmers, system or network administrators, administrators at individual departments, etc.);

d) other persons, who are under the nature of the relevant data processing under Article XIII mandated to use the personal data to perform their tasks.

2. Other authorized persons are appointed by the processing Guarantor. The condition for accepting or reassigning persons to places authorized under paragraph 1 is carried out after their prior familiarisation with this Ordinance, the Regulation and other relevant generally binding legal regulations.

3. Persons referred to in paragraph 1 of this Article are obliged to process personal data only to the extent necessary for the fulfilment of the given purpose of the personal data processing.

4. The persons referred to in paragraph 1 of this Article shall be obliged to maintain confidentiality regarding personal data and any security measures, the disclosure of which could jeopardize the personal data security. The obligation to maintain confidentiality continues even after termination of employment, studies or performance of relevant work.

Article VIII

Graduation Theses and Other Student Work

In cases where personal data would be processed in the graduation theses of students (Bachelor's, Master's, Doctoral and Dissertation), the thesis supervisor is obliged to acquaint the student with the obligations under the Regulation and this Ordinance and to ensure any further steps in accordance with this Ordinance are taken. In general, this obligation also applies to other cases where a student processes a project or performs other activities utilizing personal data. Further details may be stipulated in other internal regulations of the university or its individual constituent parts.

Part Three
Data Protection Officer

Article IX
Appointment of a Data Protection Officer

The Data Protection Officer at the university (hereafter referred to as the Officer) is appointed by the Rector on the basis of their professional qualities, in particular their expert legal knowledge and experience in the personal data protection area and their ability to perform the tasks referred to in Art. XI.

Article X

The Status 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 related to the protection and personal data processing at the university.

3. The Officer is encouraged by the university to maintain their high level of expertise and is given access to personal data, processing operations, and all the resources needed to perform tasks under Article XI.

4. The Officer is not given any specific instructions from the university regarding the fulfilment of their data protection Officer responsibilities. however, the Rector may also assign them other tasks and duties. None of these tasks or duties may lead to a conflict of interest with the position of a data protection Officer.

5. The Officer is bound by confidentiality. The obligation of confidentiality continues even after the termination of the employment relationship with the university.

6. Information about the Officer, including their contact information, is available at the public section of the university website.

Article XI
Data Protection Officer Responsibilities

1. The Officer carries out, in particular the following tasks:

   a) provides information and advice to university students and staff processing personal data and informs them of their responsibilities under this Ordinance, relevant regulations and other generally binding data protection legislation;

   b) monitors compliance with this Ordinance, the Regulation, other generally binding legislation on personal data protection and the university concepts on personal data protection, including the delegation of responsibilities, raising the awareness and organisation of training for staff involved in processing operations and related audits;

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

   d) upon request provides advice and technical assistance regarding data protection impact assessment; and monitors its application under Article 35 of the Regulation;

   e) after consultation with the persons referred to in Art. IV and V reports any personal data breach to the supervisory authority (Article 33 of the Regulation) and communicates the personal data breach to the data subject (Article 34 of the Regulation);

   f) cooperates and communicates with the supervisory authority;

   g) acts as a focal point for the supervisory authority in matters relating to the personal data processing, including prior consultation under Article 36 of the Regulation, and, where appropriate, conducts consultations on any other matters;

   h) accepts proposals from the university staff to launch new or to amend the current personal data processing and provides a statement on such proposals;

i) communicates with data subjects who can contact the Officer regarding any matters related to the processing of their personal data and the exercise of their rights under this Ordinance and the Regulation;

j) performs other tasks resulting from the Regulation, the law or other generally binding legal regulations or from this Ordinance and other university regulations.

2. The Officer supervises the university personal data processing register referred to in Art. XIII.

3. In performing their tasks, the Officer takes due account of the risks associated with the data processing activities, while taking into account the nature, scope, context and purposes of the processing.

Article XII
The Competency of the Data Protection Officer

1. If the Officer learns that a risk of a breach of the data protection policy under the Regulation, the Personal Data Protection Act, or this Ordinance, has arisen or if a breach has been detected, they are obliged to notify the appropriate Guarantor and provide a written recommendation to remove the defective or hazardous state. The Guarantor shall discuss the situation with the Officer without undue delay and, if they agree with the Officer's findings, they are obliged to refrain from further harmful or risky behaviour. The Guarantor is also obliged to take all necessary measures to prevent the situation from recurring. If the Guarantor does not agree with the Officer's recommendation, they must justify the alleged wrong conduct in writing, stating the reasons why they believe there do not constitute a breach of the rules cited in the first sentence of this paragraph or that there is no threat of a breach. In such a case, the Officer notifies the relevant persons referred to in Art. IV and V and forward the complete documentation to them.

2. If there is a threat of a breach of the rules for the personal data protection as stipulated in the Regulation, the Data Protection Act or this Ordinance or if a breach has been detected; or if no processing Guarantor has been appointed for the particular case / area of processing, the Officer is obliged to notify the relevant persons mentioned in the Art. IV and V in writing.

3. The Officer is obliged to initiate the adoption of general or individual personal data protection measures with the persons referred to in Article IV and V whenever:

a) they identify a threat of breach or detect a breach of the rules on the basis of its findings under paragraph 1 of this Article;

b) this is appropriate following the generalization of personal data protection practices.

4. The provisions of paragraphs 1 to 3 of this Article do not affect the obligation of the Officer to report (2). to report breaches of personal data security to the supervisory authority and the data subject pursuant to Art. XI 1) (e) after prior consultation of the persons referred to in Article 1 IV and V.

Part Four
University Personal Data Processing Register

Article XIII

Registration and Records of the Personal Data Processing

1. In order to monitor the personal data processing at the university, an electronic register of personal data processing activities at the university (hereinafter processing register) has been established. The Information Technology Centre (hereinafter CIT) is responsible for the operation of this processing register. The CIT director is responsible for the operation of the processing register. The workplaces and positions of the persons responsible for the operation of the processing register will be determined by the Ordinance of the CIT director.

2. The processing register is divided into two parts: Part A contains processing carried out across the university, Part B contains processing carried out by only one or several constituent parts of the university.

3. When personal data is processed within the university information systems or in connection with them, records of processing activities are kept within those systems. The CIT is responsible for the operation of whole-university information systems with the CIT director responsible for all its activities. Information systems operated only within individual constituent parts have employees designated by the Head of the constituent part as responsible for the system operation. In case of doubt whether the processing under which regime of this paragraph a particular processing falls, the Rector will decide on that matter.

4. University constituent parts wishing to introduce new personal data processing regulated by this Ordinance or to amend the current method of processing personal data (hereinafter referred to as the Proposer) notify the Officer in writing or electronically.

5. The notification referred to in the previous paragraph must contain the full description of the relevant personal data processing. If this condition is not met, the Proposer completes the notification as directed by the Officer.

6. The Guarantor always requests a prior opinion on any process implementation and establishment of any type of personal data protection solution from the Officer.

7. The Proposer can initiate new or amend the current personal data processing only after receiving an official statement form the Officer based on the result of the notification. If the statement is negative, the persons referred to in Art. IV and V are consulted.

8. New personal data processing/amendment of the current personal data processing must be recorded in the processing register.

Part Five
Principles Relating to Processing of Personal Data

Article XIV
Principles Relating to Processing of Personal Data

1. The principles relating to processing of personal data are set out in Chapter II of the Regulation. In accordance with the Regulation, personal data must be:

    a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

    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.

2. Compliance with the principles of the previous paragraph is the responsibility of the persons listed in Part Two of this Ordinance and who also must be able to evidence this compliance.

Article XV
Lawfulness of Processing

1. In accordance with Article 6 of the Regulation, processing is lawful only if and to the extent that at least one of the following applies:

    a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (the terms of the consent are detailed in Articles 7 and 8 of the Regulation);

    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 necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is in compliance with all the generally binding 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;

f) 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.

2. Paragraph 1 f) does not apply to processing carried out by the university in the performance of its tasks vested in it by the law.

3. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on generally binding applicable legislation, the Guarantor 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 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 whether personal data related to criminal convictions and offences are processed, 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 pseudonymisation.

Article XVI
Processing of Specific 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 is prohibited in cases not covered by paragraphs 2 and 3.

2. Exceptions to the prohibition on the personal data processing pursuant to paragraph 1 are set out in Article 9 of the Regulation.

3. Exceptions to the prohibition in paragraph 1 are also:

   a) data concerning health in personal records of employees and students, provided that the data were voluntarily provided by the data subject and are kept in their interest (e.g., affect the admission to studies, provision of services to persons with special needs, provision of accommodation in dormitories or calculation of the tax liability or other statutory benefits);

   b) information on membership of the unions active at the university listed in the personal and wage records of employees, provided that they were voluntarily provided by the data subject and are used for payment of membership fees or other benefits, including accounting for such payments;

   c) biometric data enabling a direct identification or authenticated of the data subject

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

4. Processing of the data defined in paragraph 1 may be carried out only with the express consent of the data subject. This consent must be given in written or electronic form and must clearly specify what data it relates to and for what purpose, and what period is given and who provides it. By signing the consent, the data subject also confirms that they have been informed of their rights. Authorized persons, who according to the nature of the relevant personal data processing under Art. VII are assigned to input and destroy the relevant data must be able to evidence the consent given for the entire period of the data processing.

5. Processing of data pursuant to paragraph 3 c) may only be used if there is a parallel option of achieving the given purpose by using other means of identification or authentication which is not dependent on biometric data and the data subject is able to choose between these means.

6. Processing of personal data which does not require identification of the data subject is regulated by Article 11 of the Regulation.

Part Six
Data Subject

Article XVII
Information Provided to the Data Subject

1. As a data controller, the university shall provide the data subject, in accordance with Article 12 of the Regulation, with all the information referred to in Articles 13 and 14 of the Regulation in concise, transparent, intelligible and easily accessible form, using clear and plain language and shall make all communications under Articles 15 to 22 and 34 of the Regulation.

2. Data subjects may contact the Officer regarding all matters related to the processing of their personal data and the exercise of their rights under this Ordinance and the Regulation.

Article XVIII
Rights of the Data Subject

Rights of the data subject to:

a) access to personal data is regulated by Article 15 of the Regulation;

b) rectification is regulated by Articles 16 and 19 of the Regulation;

c) erasure is regulated by Articles 17 and 19 of the Regulation;

d) restriction of processing is regulated by Articles 18 and 19 of the Regulation

e) data portability is regulated by Article 20 of the Regulation;

f) right to object and automated individual decision-making are governed by Articles 21 and 22 of the Regulation.

Part Seven
Publication and Security of Personal Data and Data Disclosure to Third Parties

Article XIX
Publication of Personal Data

1. Publication of personal data means their disclosure to undefined persons or groups of persons, in particular by mass media, other public communications or as part of a public list (eg, in the public domain of a university website).

2. Personal data protected under this Ordinance may be published up to the range of:

a) name and surname;

b) academic degrees;

c) photo;

d) job title at the university;

e) position in the organizational structure of the university;

f) positions held at the university;

g) university contact details (workplace address, telephone and fax number, e-mail address);

h) curriculum vitae;

i) the course of achievement of the academic qualifications;

j) share in the forms of university creative activities;

k) information about publications;

l) teaching carried out at the university;

m) academic personal web page (i.e. WWW-pages of university staff and students related to their academic or study activities at the university);

n) other data which has been made public by the data subject.

Personal data referred to in letters c), h) and m) shall be published on the basis of the consent of the data subject and to the extent specified therein.

3. The data referred to in paragraph 2 may only be published on data subjects who:

a) are university employees;

b) are university employees or students and are currently active in university self-governing or advisory bodies.

4. In the case of academic officials and university management, the publication of personal data will be regulated individually.

5. In the case of academic officials and persons currently active in university self-governing academic or advisory bodies who are not employed by the university, the publication of personal data will be regulated individually.

Article XX
Disclosure of Personal Data to Third Parties

1. Disclosure of personal data to third parties outside the university is governed by this Ordinance, the Regulation and applicable generally binding legal regulations.

2. Any disclosure of personal data to a third party outside the university which is not imposed by a generally binding legal regulation must be recorded in the processing register, including the identification details of the third party.

3. The Guarantor appointed for the given processing/area of processing is responsible for adhering to the correct procedure for disclosing personal data to third parties in accordance with this Ordinance, the Regulation and applicable generally binding legal regulations. If no Guarantor is appointed for the given processing/area of processing, the relevant persons referred to in Art. IV and V are responsible for adherence to the correct procedure.

Article XXI
Personal Data Security

1. University documents and mobile/external/portable technical information media containing personal data protected under this Ordinance shall be kept only in lockable cabinets at the university premises, or at other safe places determined by the nature of the relevant data processing under Art. XIII; or secured by encryption.

2. If the processed personal data are directly related to activities performed at the university (eg attendance sheets, answer sheets, tests, notepads, attendance lists), they are handled in the usual way to prevent personal data being misused. Other obligations set out in this Article on personal data security apply to processing of such personal data to the extent corresponding to their nature and circumstances of their usual processing.

3. Computers and other technical devices storing personal data protected by this Ordinance must be protected from unauthorized access, generally by passwords, encryption or lockdown.

4. Copies of personal data protected under this Ordinance shall be stored on technical information media in accordance with the operational rules laid down for individual data processing and stored in lockable cabinets at the university premises, or at another safe places determined by the nature of the relevant data processing under Art. XIII; or secured by encryption. They must be stored in a room other than the room the original data is stored in.

5. In the event that a Guarantor, an authorized person or a university employee suspects that a personal data breach might occur or detects a breach, they are obliged to notify the Officer immediately.

6. Reporting of personal data breaches to the supervisory authority (Art. 33 of the Regulation) and communication of a personal data breach to the data subject (Art. 34 of the Regulation) shall be carried out by the Officer after prior consultation with the persons referred to in Art. IV and V.

Part Eight
Final Provisions

Article XXII
Final Provisions

1. This Ordinance repeals the USB Rector's Ordinance No. 46 on implementation of Act no. 101/2000 Coll., On Personal Data Protection and on Amendments to Some Acts.
2. Compliance with this Ordinance is monitored by the Data Protection Officer.
3. This Ordinance becomes effective on the date of its signature on 21 May 2018.

Assoc.Prof. Tomáš Machula PhD, Th., m.p.
Rector

Revised by: Mgr.Jan Černý

Distribution: members of the USB management, Deans of faculties, Directors of other constituent parts of the USB, faculty secretaries, managerial employees Rectorate departments