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

Ref. no: R 378 Date: 17 May 2018

Rector's Ordinance
laying down the rules for the protection and processing of personal data

Pursuant to the provisions of Section 10, par. 1 of Act No. 111/1998 Coll., regulating Higher Education Institutions and on Amendments and Supplements to some other Acts (the Higher Education Act), as amended, (hereinafter "the Act"), and the provisions of Art. 14 of the Statute of the University of South Bohemia in České Budějovice (hereinafter referred to as the "University"), I hereby issue the following Ordinance:

Part One
Basic Provisions

Article I
Scope

1. The present Ordinance lays down the principles and rules for the processing of personal data at the University, also laying down the responsibility of persons ensuring the protection of personal data at the University, defining the rights and obligations of employees, students or other natural persons and legal entities involved in activities related to the processing of such data.

2. The present Ordinance covers all processing of personal data carried out by employees and students of the University in the fulfilment of their job duties or school curriculum, as well as any processing carried out by other natural persons or legal entities processing personal data under an agreement with the University.

3. This Ordinance follows from Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 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 "the Regulation"), as well as from Act No. 101/2000 Coll. on the protection of personal data and amending certain acts, as amended (hereinafter "Act on the Protection of Personal Data"), whereas it complements and elaborates on some of their provisions to regulate relationships inside the university and lays down respective organisational measures.

Article II
Interpretation of selected terms

1. For the purposes of the present ordinance, the following apply:

   a) "Personal data" refers to any information relating to an identified or identifiable natural person (hereinafter the data subject); an identifiable natural person is a natural person who can be identified, either directly or indirectly, by reference to an identifier such as their name, an identification number, location data, a network identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

   b) "personal data processing" refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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) "the controller" refers to any natural or legal person, public authority, agency or other body which, on its own 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) a "processor" refers to any natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller;

   e) "profiling" refers to any form of automated processing of personal data consisting of their use for assessing certain personal aspects relating to a natural person, particularly to the analysis or estimate of aspects regarding his or her work performance, economic situation, health condition, personal preferences, interests, reliability, behaviour, location or movement;

   f) "pseudonymisation" refers to 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) a "filing system" means any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

   h) a "recipient" refers to a natural or legal person, public authority, agency or another body to which personal data are disclosed, whether such recipient is a third party or not. However, public authorities which may receive personal data within 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) a “third party” refers to any natural or legal person, public authority, agency or any other body other than the data subject, controller, processor or persons who, under the direct authority of a controller or processor, are authorized to process personal data;

j) “consent” refers to any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, through a statement or through a clear and affirmative action, signifies their agreement to the processing of personal data relating to him or her;

k) a “personal data breach” refers to 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” refers to 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” refers to 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 data on the provision of health care services which reveal information about his or her health status.

2. Other terms used to refer to the processing and protection of personal data are given in Art. 4 of the Regulation, or, as the case may be, in the text of or in attachments to the present Ordinance, where expedient.

Part two
Responsibility of persons ensuring the protection of personal data

Article III
Position of the University

The University is the entity responsible for the processing of personal data given in Art. I, par. 2 of the present Ordinance. Depending on the specific circumstances, the University may act both as the controller and the processor. Part two of the present Ordinance sets out persons participating in the protection of personal data, as required by the Regulation and the Act on the Protection of Personal Data.

Article IV
Central level

1. The Rector’s position is stipulated by the Act, the University Statute and other internal regulations of the university. The Rector acts as the governing body of the University responsible for the adherence to principles, rules and procedures for the processing of personal data coming in and

out of the University, in cases implemented at the central level of the University, as well as in cases where responsibility was not transferred to other persons given in this part.

2. The Bursar is accountable to the Rector of the University for observing the principles, rules and procedures for processing personal data implemented within the Bursar's competences and for activities under Art. 3, par. 3 and Annex No. 2 of the Organisational Rules of the University Rectorate.

3. Vice-Rectors are accountable to the Rector of the University for observing the principles, rules and procedures for processing personal data implemented within the Vice-Rectors´ competences and for activities under Art. 3, par. 2 and Annex No. 2 of the Organisational Rules of the University Rectorate.

Article V
Heads of constituent parts of the USB

1. Deans of respective faculties of the University are accountable to the Rector for observing the principles, rules and procedures for processing personal data implemented by employees and students of each respective faculty of the University in the fulfilment of their job duties or school curriculum, as well as for any other natural persons or legal entities processing personal data under an agreement with the faculty of the University in matters vested in it under the provisions of Section 24 of the Act, Art. 15 of the Statute of the University, other internal regulations and other University regulations.

2. Heads of Units for educational and creative activities or for the provision of information services within the meaning of Art. 12, par. 3 of the Statute of the University (hereinafter the "University unit") are accountable to the Rector for observing the principles, rules and procedures for processing personal data implemented by employees and students of each respective faculty of the University in the fulfilment of their job duties, and are also responsible for observing such principles, rules and procedures by other natural persons or legal entities processing personal data under an agreement with the University unit in matters vested in it by the internal regulations of the University or the University unit.

3. Directors of facilities for cultural and sports activities, accommodation and catering or facilities ensuring the operations of the University within the meaning of Art. 12, par. 4 of the Statute of the University (hereinafter "specialised units") are accountable to the Rector for observing the principles, rules and procedures for processing personal data implemented by employees of specialized units, as well as for any other natural persons or legal entities processing personal data under an agreement with the facility for a particular purpose in matters vested in it by the internal regulations of the University or the facility for a particular purpose.

Article VI
Guarantor of personal data processing

1. In order to ensure the protection of personal data and their processing are in compliance with the Regulation and the Act on the Protection of Personal Data, Guarantors of personal data processing are appointed for each respective type or area of processing (hereinafter "Guarantor").

2. A Guarantor is a person responsible for adherence to the principles, rules and procedures (laid down in this Ordinance, Regulation and other relevant generally binding legal regulations) for the

processing of personal data implemented within their assigned type or area of processing. The Guarantor is responsible for the above-mentioned activities as of their appointment until the termination of their activities, including safe data archiving.

3. Within each assigned type/area of processing, the Guarantor shall carries out a data protection impact assessment under Art. 35 of the Regulation. For this purpose, the Guarantor shall request the opinion of the Data Protection Officer.

4. For specific types/areas of processing under part A of the data processing register of the University (see Art. XIII, par. 2 of the present Ordinance), the Rector is going to appoint Guarantors with university-wide competence.

5. For specific types/areas of processing under part B of the data processing register of the University (see Art. XIII, par. 2 of the present Ordinance), the Heads of the constituent parts are going to appoint Guarantors with competence limited to the specific constituent part.

6. In cases of ongoing processing of personal data, the Guarantor shall be appointed no later than ten days after the effective date of the present Ordinance. For newly-introduced processing, the Guarantor shall be appointed prior to the commencement of the processing.

7. Persons listed in paragraphs 4 and 5 of the present Article must inform the data protection officer on the appointment of the Guarantor without delay.

Article VII
Other authorized persons

1. Other authorised persons may handle the personal data:

   a) persons authorised with entering and disposing of personal data in keeping with the characteristics of the processing under Art. XIII;

   b) persons who are superiors to the persons given in a) with regard to organisational hierarchy or methodology;

   c) persons ensuring the organisational, functional and technical administration of the respective type of data processing (usually analysts, programmers, and network administrators, administrators at respective units, etc.);

   d) other persons authorised to use such personal data in order to fulfil their tasks, pursuant to the characteristics of each particular data processing pursuant to Art. XIII.

2. Other authorised persons are appointed by the Guarantor of processing. Persons may be recruited or transferred to positions with authorisation under paragraph 1 only after being demonstrably acquainted with the present Ordinance, the Regulation and other relevant generally binding legal regulations.

3. Persons listed in par. 1 of the present article are obliged to process personal data only in the extent required to fulfil the purpose of such processing.

4. Persons given in par. 1 of the present article are obliged to observe confidentiality on personal data and on those safety measures the disclosure of which might put Personal data security at risk. The confidentiality obligation continues beyond the term of employment, studies or performance of respective work.

Article VIII
Theses and other student papers

In cases when personal data are being processed in student theses (bachelor, master´s, advanced master´s and dissertation theses), the thesis supervisor is obliged to inform students about the obligations ensuing from the Regulation and the present Ordinance and to ensure any other steps in compliance with the present Ordinance. In general, this obligation also applies to other cases when a student is working on a project or other activities which entail personal data processing as part of their curriculum. Other details may be laid down by other internal regulations of the University or its constituent parts.

Part three
Data Protection Officer

Article IX
Appointing the Data Protection Officer

The University Data Protection Officer (hereinafter "Officer") is appointed by the Rector based on professional competence, in particular in relation to expert knowledge in the field of law and practical applications in personal data protection, as well as the ability to fulfil the tasks given in Art. XI.

Article X
Position of the Officer

1. The Officer is an employee of the University and reports directly to the Rector.

2. The Officer is involved in all the processes and matters regarding the protection and processing of personal data at the University.

3. The Officer is assisted by the University in maintaining their expertise and is granted access to personal data, processing operations and any other resources the Officer may need to fulfil the tasks under Art. XI.

4. The Officer is not given any specific instructions regarding the fulfilment of their tasks by the University. That stated, the Rector may assign the Officer with other tasks and obligations. However, such tasks must not lead to any conflict of interest with the position of the Officer.

5. The Officer is bound by the obligation of confidentiality regarding the performance of the Officer´s tasks. The confidentiality obligation continues after the termination of the employment relationship with the University.

6. Details of the Officer, including contact information, are provided in the public section of the University's website.

Article XI
Officer's Responsibilities

1. In particular, the Officer performs the following tasks:

   a) provides information and consultancy to students and members of staff of the University who process personal data regarding their obligations under the present Ordinance, the Regulation and other generally binding data protection legal regulations;

   b) monitors compliance with this Ordinance and the Regulation with other generally binding data protection legal regulations and with the policies of the University in relation to the protection of personal data, including the assignment of responsibilities, raising awareness and training of staff involved in processing operations and the related audits;

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

   d) when requested to do so, provides consultancy and professional assistance regarding data protection impact assessments and monitors its implementation pursuant to Art. 35 of the Regulation;

   e) after prior consultation with the persons given in Art. IV and V, reports any cases of personal data breaches to the supervisory authority (Art. 33 of the Regulation) and communicates cases of personal data breaches to the data subject (Art. 34 of the Regulation);

   f) cooperates and communicates with the supervisory authority;

   g) serves as a point of contact for the supervisory authority on issues relating to personal data processing, including prior consultation under Article 36 of the Regulation, and organises consultation, where appropriate, with regard to any other matters;

   h) receives proposals from University members of staff regarding the commencement of new data processing or any changes to existing data processing and issues opinions regarding such proposals;

   i) communicates with data subjects who may approach the Officer regarding any matters related to the processing of their data and the exercising of their rights under the present Ordinance and Regulation;

   j) fulfils other tasks required by his/her position ensuing from the Regulation, the Act or other generally binding legal regulations, or from this Ordinance and other University policies.

2. The Officer supervises the operation of the data processing register of the University as set out in Art. XIII.

3. The Officer shall give due consideration to the risks associated with data processing activities, also taking into account the nature, scope, context and purposes of processing.

Article XII
Area of responsibility of the Officer

1. Should the Officer learn that there is a risk of a data protection breach regarding the rules ensuing from the Regulation, the Act on the Protection of Personal Data or the present Ordinance or, in case a breach has been established, the Officer is obliged to notify the respective Guarantor and make a written recommendation on how to rectify the harmful or risky situation. The Guarantor shall discuss the situation with the Officer in due time and if the Guarantor agrees with the findings made by the Officer, the Guarantor is obliged to refrain engaging in any other harmful or risky conduct. The Guarantor is also obliged to take necessary measures to prevent the recurrence of the situation. If the Guarantor does not agree with the recommendation made by the Officer, the Guarantor must provide written justification of the questioned conduct and give reasons on why they think the rules given in the first sentence were not breached, or why there is no risk of any breach of these rules. In such a case, the Officer shall report such fact to the competent persons provided in Arts. IV and V and refer the documentation to such competent persons.

2. If there is a risk of a data protection breach regarding the rules ensuing from the Regulation, the Act on the Protection of Personal Data or the present Ordinance or, in case the breach has been established and there is no Guarantor appointed for the type/area of processing, the Officer is obliged to notify the respective competent persons provided in Arts. IV and V.

3. The Officer is obliged to suggest the adoption of general or specific data protection measures to those persons given in Arts. IV and V, whenever:

   a) based on the Officer's findings under par 1 of this Article, the Officer finds out that there is the potential for or has been an actual data protection breach;

   b) it is appropriate in relation to general practice in the field of personal data protection.

4. The provisions of paragraphs 1 to 3 of the present Article are without prejudice to the Officer's obligation to, after prior consultation with the persons given in Arts. IV and V, report a data protection breach to the supervisory authority and to the data subject pursuant to Article XI, 1 e).

Part four
Data processing register of the University

Article XIII
Registering and filing of personal data processing

1. In order to keep track of the personal data processing at the University, an electronic register of data processing activities at the University shall be established (hereinafter the "processing register"). The Information Technology Centre (ITC) is in charge of the operation of this processing register. The ICT Director is responsible for the operation of the processing register. The units and functions of persons ensuring the operation of the processing register shall be laid down in an ordinance issued by the ICT Director.

2. The processing register shall be divided into two parts: Part A lists the university-wide types of processing while part B lists the types of processing carried out by one or more constituent parts of the University.

3. For types of data processing within the University information systems or in connection with these systems, records of processing activities are kept as part of these systems. The ITC is in charge of the operation of university-wide information systems. The ICT Director is responsible for the activities of these systems. Employees authorised by the head of each respective unit are in charge of the operation of information systems operated only as part of the individual constituent parts of the University. Where there is doubt as to whether the processing falls under the arrangement pursuant to this paragraph, the Rector shall decide upon the issue.

4. The constituent parts of the University which intend to introduce a new type of data processing protected under the present Ordinance, or, in case they intend to change an existing type of data processing (hereinafter a "Proponent") shall notify the Officer of this fact in writing or in electronic form.

5. The notification pursuant to the previous paragraph must contain the entire characteristics of the proposed data processing. If this condition is not met, the Proponent shall add details to the notification as instructed by the Officer.

6. The Guarantor shall always ask for the previous opinion of the Officer on the implementation procedure and the features of the solution for the protection of processed personal data.

7. The Proponent is entitled to commence a new type of data processing or change an existing type of data processing only after receiving an official opinion by the Officer based on the result of the notification. If the opinion is negative, the matter shall be consulted with the persons given in Articles IV. and V.

8. New data processing, i.e. a change to the existing personal data processing, must be recorded in the processing register.

Part five
Principles relating to the processing of personal data

Article XIV
Principles relating to the processing of personal data

1. Principles relating to the processing of personal data are given in Chapter II of the Regulation. Pursuant to the Regulation:

   a) the personal data must be processed in a lawful, proper and transparent manner;

   b) personal data must be collected for specified, explicit and legitimate purposes and they must not be further processed in any manner incompatible with those purposes;

   c) personal data must be adequate, relevant and limited to the scope necessary for the purposes for which they are being processed;

   d) personal data must be accurate and updated as necessary; every reasonable step must be taken to ensure that personal inaccurate with regard to the processing purposes are erased or rectified without delay;

e) personal data must be stored in a form enabling the identification of data subjects for no longer than what is necessary for the processing purposes;

f) personal data must be processed in a manner ensuring appropriate personal data security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;

2. The persons provided in Part two of the present Ordinance are responsible for compliance with the principles laid down in the previous paragraph and must be able to demonstrate such compliance in court.

Article XV
Lawfulness of processing

1. Pursuant to Article 6 of the Regulation, data processing is lawful only if at least one of the following conditions is met and only to the appropriate 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 for expressing consent are given in detail in Arts. 7 and 8 of the Regulation);

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing complies with the applicable generally binding legal regulations to fulfil the legal obligations of the controller;

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

e) processing complies with the applicable generally binding legal regulations necessary for the performance of a task being carried out in the public interest or in the exercise of public authority vested in the controller;

f) processing is required to protect the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject which require the protection of personal data, especially where the data subject is a child.

2. Paragraph 1 f) does not apply to the processing of personal data carried out by the University in cases when the University is acting as public authority in matters vested in it by law.

3. If the data are processed for a purpose other than the one for which the data was collected and is not based on the consent of the data subject or other applicable generally binding legal regulations, the Guarantor shall, in order to establish whether the processing for a different purpose is compatible with the original purposes of data collection, take into account the following:

a) any connection between the original purposes of the collection of the personal data and the purposes of the intended further processing;

b) circumstances of the personal data collection, particularly with regard to the relationship between the data subjects and the University;

c) the nature of personal data, particularly as to whether the processing involves special categories of data under Art. 9 of the Regulation or personal data regarding criminal convictions and offences under Art. 10 of the Regulation;

d) 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 special categories of personal data

1. It is prohibited to process any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or to process genetic data or 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 in cases which are not covered by paragraphs 2 and 3;

2. Exemptions from the ban on personal data processing under paragraph 1 are given in Article 9 of the Regulation.

3. Exemptions from the ban under paragraph 1 include, without limitation:

   a) data on health condition contained in the personal records of employees and students in filing systems under the condition that these data were provided by the data subjects to the filing system in question voluntarily and are maintained in their favour (e.g. they affect their admission to the University, the provision of services to persons with specific needs, accommodation in residential halls or the calculation of due tax or other statutory allowances);

   b) data on membership in organisations operating at the University contained in the personal and salary records of employees in case they were provided by the data subjects to the filing system in question voluntarily and are intended for the payment of membership fees or other allowances, including accounting records on these payments;

   c) biometric data enabling the direct identification or authentication of the data subject;

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

4. Processing of data defined under paragraph 1 may only take place subject to explicit consent being given by the data subject. Such consent must be given in writing or in electronic form and it must clearly state which data it concerns, for what purpose, for what period and by whom the consent is provided. By signing the consent, the data subject confirms being previously advised of their rights. Authorised persons who are entrusted with entering and disposing of the given data depending on the characteristics of the respective data processing under Art. VII are obliged to

be able to demonstrate the existence of such consent throughout the entire period of their processing.

5. Data processing under paragraph 3 c) may only be used if there is an alternative option to achieve the given purpose in parallel using other means of identification or authentication which does not depend on biometric data, and the data subject shall have the possibility to choose one of these alternatives.

6. Data processing not requiring data subject identification is governed by Art. 11 of the Regulation.

Part six
Data subject

Article XVII
Information provided to the data subject

1. As a controller and in compliance with Art.12 of the Regulation, the University provides all the information given in Arts. 13 and 14 of the Regulation to the data subject in a brief, transparent, comprehensible and easily accessible manner using clear and simple language, and needs to satisfy all communications under Articles 15 to 22 and under Article 34 of the Regulation on processing.

2. Data subjects who may approach the Officer regarding any matters related to the processing of their data and the exercise of their rights under the present Ordinance and Regulation.

Article XVIII
Rights of the Data Subject

Each data subject has the following rights:

a) The right of access to personal data governed by Art.15 of the Regulation;

b) The right to rectification governed by Arts. 16 and 19 of the Regulation;

c) The right to erasure governed by Arts. 17 and 19 of the Regulation;

d) The right to restricting processing governed by Arts. 18 and 19 of the Regulation;

e) The right to data portability governed by Art. 20 of the Regulation;

f) The right to object to automated individualised decision-making, which is governed by Arts. 21 and 22 of the Regulation.

Part seven
Publication and personal data security and their disclosure to third parties

Article XIX
Publication of Personal Data

1. The publication of personal data refers to their disclosure to indeterminate people or to an indeterminate group of people, particularly by means of mass media, other public communication or as part of a public list (such as in the public section of the University's website).

2. Personal data protected under the present Ordinance may only be published in the following scope:

   a) name and surname;

   b) academic titles;

   c) photograph;

   d) job position at the University;

   e) position in the University organisational chart;

   f) positions held at the University;

   g) contact details related to the University (University unit addresses, phone and fax numbers, e-mail addresses);

   h) CV;

   i) course of academic qualifications;

   j) contribution to specific forms of University creative activities;

   k) information on published publications;

   l) teaching at the University;

   m) personal academic websites (i.e. websites of employees and students of the University related to their academic or scholarly activities at the University);

   n) any other data which the data subject has published about themselves.

   Personal data given under letters c), h) and m) shall be published subject to consent being given by the data subject and in the scope set out in such consent.

3. The data given in paragraph 2 may only be published about data subjects who:

   a) are employees of the University;

b) are employees or students of the University and are currently active in self-governing academic or advisory bodies of the University.

4. For persons holding academic positions and heads of constituent parts of the University, the publication of personal data shall be provided for individually.

5. For persons holding academic positions and persons currently active in self-governing academic or advisory bodies of the University who are not in an employment relationship with the University, the publication of personal data shall be provided for individually.

Article XX
Disclosure of personal data to third parties

1. The disclosure of personal data to third parties outside of the University is governed by the present Ordinance, the Regulation and the applicable generally binding legal regulations.

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

3. The Guarantor appointed for each specific case/area of processing is responsible for adhering to the correct procedure for the disclosure of personal data to third parties outside of the University in compliance with this Ordinance, the Regulation and the applicable generally binding legal regulations. If there is no Guarantor appointed for the given case/area of processing, the respective competent persons given under Arts. IV and V. shall be responsible for adhering to the correct procedure for the disclosure of personal data to third parties outside the University.

Article XXI
Personal data security

1. Written documents and mobile/external/portable technical data carriers at the disposal of the University containing personal data protected under the present Ordinance must only be stored in lockable cases within University premises or in other safe premises corresponding to the nature of the processing of the personal data in question pursuant to Art. XIII or secured by encryption.

2. If personal data concerning activities performed at the University are processed (such as attendance sheets, response sheets, tests, notepads, attendance list), they shall be secured following typical procedures to prevent the risk of personal data misuse. Other obligations set out in this Article shall apply to the processing of such personal data only in the scope corresponding to their nature and the circumstances of their usual processing.

3. Computers and other technical devices used to save data containing personal data protected under this Ordinance must be secured to prevent free access by unauthorised persons. As a rule, this is done by employing access passwords, encryption or locking.

4. Copies of personal data protected under the present Directive must only be saved on technical information carriers pursuant to the operational rules laid down for specific types of data processing and stored in lockable cases within University premises or in other safe premises corresponding to the nature of the processing of the personal data in question pursuant to Art.

XIII or secured by encryption. They must always be stored in a different room than the original data.

5. In case the Guarantor, the authorised person or an employee of the University ascertain or suspect that a personal data breach has occurred or might occur, the Guarantor is obliged to report this to the Officer without delay.

6. Reporting any cases of personal data breaches to the supervisory authority (Art. 33 of the Regulation) and communicating cases of personal data breaches to the data subject (Art. 34 of the Regulation) shall be carried out after prior consultation with the persons provided in Arts. IV and V by the Officer.

Part eight
Final Provisions

Article XXII
Final Provisions

1. The present Ordinance repeals Rector's Ordinance for the USB no. 46 implementing Act no. 101/2000 Coll on personal data protection, amending certain acts.

2. Supervision over compliance with the present Ordinance shall be carried out by the Officer.

3. This directive comes into force on the date of its signature and becomes effective on 21 May 2018.

Doc. Tomáš Machula, Ph.D., Th.D.
Rector

Prepared by: Mgr. Jan Černý

Distribution list: members of management, Deans of USB faculties, Directors of non-faculty constituent parts, faculty secretaries, managerial employees of Rectorate units