Organizational and Technical Measures to Achieve and Demonstrate Compliance with GDPR

Revised as of March 31, 2021.

Modifications as of March 31, 2021:
Inserted a new point 10) Rules for making audiovisual recordings of state final examinations, state doctoral examinations and presentations and defenses of final theses

- Recording of a distance state final examination, a state doctoral examination or a presentation and defense of a final thesis held without the presence of the public (hereinafter referred to as **Record**) is the fulfillment of obligations pursuant to Section 95c (1) (c) under the Higher Education Act, as amended.
- Rules are set for the obtaining, access and storage and security of Records

These Organizational and Technical Measures for Achieving and Demonstrating Compliance with the GDPR follow the Rector's Directive No. 5/2018 on Protection and Processing of Personal Data (hereinafter referred to as **Directive**).

1) Implementation of a system for storing and securing spare keys from offices and storage areas and a system for recording issued keys
Who is responsible: OSM (Protection and Security of VŠE Property)
Valid from: October 31, 2018

2) Introduction of a system of registration of "anonymous" identification cards
Who is responsible: OSM (Protection and Security of VŠE Property)
Valid from: October 31, 2018

3) Prevent the transmission of unsecured documentation containing personal data by e-mail outside VŠE (including redirected mail). To use a secure method for transmission that does not allow access by unauthorized persons, e.g., via a data box or in an encrypted file via e-mail. *Who is responsible:* employees of VŠE
Valid from: October 1, 2018

4) Ensure that data files with personal data on portable electronic data carriers (notebook, mobile phone, external drive, flash drive, etc.) are password protected against file opening. The preferred variant is to encrypt and password protect the entire electronic data carrier (typically for a laptop).
Who is responsible: employees of VŠE
Valid from: October 31, 2018

5) Computers on which personal data are processed must meet the following minimum-security requirements:
   - Regular, preferably automated, security updates of the operating system and installed programs,

- each computer user uses their password-protected account, or in a comparable or more secure way of user authentication (biometric data, chip card, ..),
- the user uses a resident antivirus program that regularly updates spyware and virus definitions

Who is responsible: employees of VŠE
Valid from: April 1, 2019

6) Computers in school classrooms and computers in offices connected to a fixed network must also meet the following security requirements:
   - a school image is installed on the computer (a Windows school installation prepared by the Informatics Center or the Information Technology Center at the Faculty of Management),
   - the computer is registered in the school directory service (Active Directory); user accounts in Active Directory are used for login,
   - an antivirus program administered by the Informatics Center or the Information Technology Center at the Faculty of Management is installed on the computer.

   One or more conditions may not be met if technical reasons prevent it, for example, a school image with Windows will not be installed on Apple Mac computers. These exceptions must be registered at the Help Desk Section of the Informatics Center.
   Who is responsible: employees of VŠE
   Valid from: April 1, 2019

7) When processing the personal data on the basis of the consent of the personal data subject
   - consent must always be obtained as a separate document, separate from other communications and information. The personal data subject will always receive a copy of the granted consent, including information on the method of revoking the granted consent
   - use only the uniform text of the VŠE consent (available from the Commissioner for Protection of Personal Data of VŠE)
   - for the processing of sensitive personal data (biometric data, photographs, audio, video, health status, social status, racial or ethnic origin, etc.), it is always necessary to grant a separate consent, separate from other consents
   - introduction of records of granted and revoked consents at the VŠE Commissioner

   Who is responsible: employees of VŠE
   Valid from: October 1, 2018

8) In the case of processing sensitive personal data (special category of personal data according to GDPR) for the purposes of scientific research, it is necessary to meet at least the following facts:
   - processing impact assessment (performed by the Commissioner for Protection of Personal Data of VŠE)
   - if a legitimate purpose is documented, the personal data may be processed without the consent of the subject
   - it is necessary to include this activity in the Records Register. The Contact Person is responsible for the inclusion
   - all those involved in the processing will sign an obligation of confidentiality (uniform text available from the Commissioner for

Protection of Personal Data of VŠE)
- communicate the necessary information to the data subject before starting the processing (information will be provided by the Commissioner for Protection of Personal Data of VŠE), including proof of scope from a minimization perspective
- the documentation of the processing of sensitive personal data is stored with the Commissioner for Protection of Personal Data of VŠE

Who is responsible: employees of VŠE
Valid from: October 1, 2018

9) Introduction of a "clean desk" policy for documents containing personal when leaving the workplace
Who is responsible: employees of VŠE
Valid from: October 1, 2018

10) Audiovisual recording of a state final examinations, state doctoral examinations and presentations and defenses of final theses

Defining the purpose of recording:
Recording of a distance state final examination, a state doctoral examination or a presentation and defense of a final thesis held without the presence of the public (hereinafter referred to as **Record**) is the fulfillment of obligations pursuant to Section 95c (1) (c) under the Higher Education Act, as amended.
Use the tools of the distance method of communication in the state examination and conduct it without the presence of the public, provided that it obtains an audiovisual Record of its course, which it retains for a period of 5 years; the higher education institution shall provide the Record only to a public authority in the exercise of its powers, at its request.

Rules for obtaining:

- The Ministry of Education, Youth and Sports will declare an extraordinary event by its decision and enable this recording
- The Dean allows the state examination or the presentation and defense to be held remotely
- The state exam is not public

Rules for accessing the Record:

- if the data subject (student, member of the commission) requests a copy of the record, the faculty will provide a copy of the Record, provided that other persons on the Record must provide written consent to the processing of personal data, or must be anonymized,
- the Record may be made available to the public authorities who request it and must state the relevant reason.

Rules for storing Records:
- Immediately remove the Record from Stream (from Office 365) and delete the unencrypted Record in Office 365,
- encrypt the file of the Record; assign a separate password for each Record, which cannot be derived from the student's identification,
- the Record must be securely stored for 5 years, in duplicate, then deleted,
- measures must be taken to prevent unauthorized persons from accessing the Record,

- save the Record to two different repositories, such as Office 365 and an external drive.
- store passwords for individual records in a suitable password manager,
- the person who will have access to the encrypted records will have substitutability and will be registered with the secretary of the faculty

Who is responsible: employees of VŠE
Valid from: February 1, 2021

11) All published documentation (text, audio, video, photo) will be anonymized to the extent ensuring the minimization of published personal data, including signatures. Anonymization does not have to be carried out if the publication of the personal data is made possible by law or is supported by another authorization to publish the personal data (e.g., by consent). Ambiguities must be consulted with the Commissioner for Protection of Personal Data of VŠE
Who is responsible: employees of VŠE
Valid from: October 1, 2018

12) When obtaining photographic, audio or video documentation from events held on the premises of VŠE, ensure that participants are informed about the obtaining of documentation and the purpose of this obtaining.
Who is responsible: employees of VŠE
Valid from: October 1, 2018

13) When obtaining photographic or video documentation from public events, ensure that participants are informed about obtaining of this documentation for the purpose of publication on the VŠE website. Make sure to mark the employees obtaining the documentation visibly and prominently
Who is responsible: employees of VŠE
Valid from: October 1, 2018

14) Ensuring the legal basis for publishing of personal data (photo, text, video, audio) on a social media network, or ensuring their anonymization or deletion. In case of ambiguity, the suitability, adequacy and legitimacy of a specific publication should always be assessed by the Commissioner for Protection of Personal Data of VŠE
Who is responsible: employees of VŠE
Valid from: October 1, 2018

15) When concluding contracts (amendments) on the processing of personal data, ensure the responsibility of the processor in dealing with the personal data (subject and time of processing, nature and purpose of processing, type of personal data, duties and rights of controller and processor, obligation of confidentiality, cooperation in exercising rights of the subject of the personal data and others). At the same time, define electronic communication primarily through the address dpo@vse.cz
Who is responsible: employees of VŠE
Valid from: December 31, 2018

16) Physical documentation containing personal data must be kept in lockable offices and lockable storage areas with access only for authorized personnel.
Who is responsible: employees of VŠE
Valid from: October 1, 2018

17) If the physical documentation containing the personal data is not kept in lockable storage areas, access of other persons (e.g., cleaning, repairs, visits, etc.) must be ensured only in the company of an authorized person
Responsible: VŠE employees
Valid from: October 1, 2018

18) Revision of all documents containing personal data on hard disks and network folders and bringing these documents into compliance with the legality for processing. Ambiguities must be consulted with the Commissioner for Protection of Personal Data of VŠE
Who is responsible: employees of VŠE
Valid from: December 31, 2018

19) Revision of all documents containing personal data in their e-mail boxes and ensuring that these data are brought into compliance with the legality for processing. Ambiguities must be consulted with the Commissioner for Protection of Personal Data of VŠE
Who is responsible: employees of VŠE
Valid from: December 31, 2018

20) Violation of protection of personal data (defined by the methodological procedure of VŠE) is always reported immediately to the Help Desk Section of the Informatics Center
Who is responsible: employees of VŠE
Valid from: October 31, 2018

21) The loss or theft of an electronic data carrier (laptop, external disk, mobile phone, flash disk, etc.) in which the personal data were stored is always reported immediately to the Help Desk Section of the Informatics Center.
Who is responsible: employees of VŠE
Valid from: October 31, 2018

22) Suspicion of theft or misuse of access data to information systems is always reported immediately to the Help Desk Section of the Informatics Center.
Who is responsible: employees of VŠE
Valid from: October 31, 2018

23) Acquaintance of new employees with regulations in the field of personal data protection:
- Directive
- Organizational and Technical Measures to Achieve and Demonstrate Compliance with GDPR (i.e., this document)

Who is responsible: Informatics Centre
Valid from: April 1, 2019

24) Training/acquaintance of employees with changes in the field of personal data protection during the revision of the following documents:
- Directive
- Organizational and Technical Measures to Achieve and Demonstrate Compliance with GDPR (i.e., this document)
- Procedure for Reporting a Breach of Personal Data Protection by an Employee.

Who is responsible: Informatics Centre
Valid from: April 1, 2019

25) If another person ("non-employee", e.g., an external person or a student on a project) processes personal data, this particular person must be informed with regulations in the field of personal data protection and must sign the Data Protection Statement (see Annex). The signed Data Protection Statements are handed over to the Informatics Center via Help Desk workplaces.
This does not apply to cases where the protection of personal data is addressed by contract.
Responsible: VŠE employee who provided access to the personal data.
Valid from: April 1, 2019

26) Implementation of the process of regular testing, assessment and evaluation of the effectiveness of the implemented organizational and technical measures and compliance with the Directive
Responsible: Director of the Informatics Center
Valid from: January 1, 2019

27) Periodic quarterly inspection of the topicality and completeness of the Records Register of the VŠE personal data, including the transmission of information on its implementation to the Commissioner for Protection of Personal Data.
Responsible: components of VŠE through authorized persons (see Directive)
Valid from: April 1, 2019

Milan Nidl
March 31, 2021

Data Protection Statement

Mr / Ms: …….....

Username at VŠE .....

(hereinafter referred to as **Individual**) is involved in work, study or scientific activities within VŠE, which also includes the processing of personal data. The Individual shall be obliged to comply with applicable laws governing the protection of personal data and the Directive of VŠE, on Protection and Processing of Personal Data (hereinafter referred to as **Directive**). The Individual has been acquainted with the Directive, as well as with the Organizational and Technical Measures to Achieve and Demonstrate Compliance with GDPR adopted by VŠE in Prague in connection with the protection and processing of personal data.

When dealing with personal data, the Individual shall be obliged to observe the following rules in particular:

1) limit the collection or access to personal data to the necessary legitimate minimum necessary to achieve the primary purpose of data collection;
2) to protect personal data, as well as access to them, at the time the Individual has them at their disposal, has been entrusted to them or otherwise made available to them, from illegal or illegitimate access or use;
3) maintain confidentiality regarding the personal data and the procedures used to protect them;
4) immediately notify VŠE of any suspicion of a breach of the integrity or protection of personal data in accordance with the provisions of the VŠE Directive.

The Individual hereby acknowledges that, by violating the obligations arising from the relevant legal regulations on personal data protection or VŠE Directive, the Individual may cause VŠE or third parties damage, for which the Individual may be held liable, including legal liability.

In …… Date……

Individual's signature……..