

JAMU



JOURNAL

Year 2018

part published on 20 December 2018

CONTENTS:

50. Directive on Personal Data Protection (valid as of 20 December 2018, effective as of 1 January 2019)

DIRECTIVE
of 20 December 2018
on Personal Data Protection

The Rector issues the following Directive:

PART ONE
GENERAL PROVISIONS

Art. 1

Subject and Purpose

(1) This Directive

- a) stipulates principles and rules of personal data protection at JAMU,
- b) stipulates the responsibilities of persons in charge of personal data protection,
- c) defines rights and duties of employees and, as the case may be, other natural and legal persons participating in activities associated with the processing of personal data.

(2) The purpose of this internal regulation is to adopt and introduce adequate technical and organizational measures to ensure the protection of personal data in compliance with Art. 24 et seq. Regulation (EC) No. 2016/679 of the European Parliament and the Council on the protection of individuals 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),

Art. 2

Definition of Certain Terms

For the purposes hereof,

- a) GDPR means Regulation (EC) No. 2016/679 of the European Parliament and the Council on the protection of individuals 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).
- b) personal data means any information on an identified or identifiable natural person (hereinafter referred to as the "Data Subject"); an identifiable natural person is a person that may be directly or indirectly identified, mainly through reference to a certain 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,
- c) sensitive data means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation,
- d) Employer is Janáček Academy of Music and Performing Arts in Brno,
- e) Controller is the Employer in case
 1. it determines the purpose and means of personal data processing,
 2. it is referred to as Controller by a special law,
- f) Processor is the Employer in case it is entitled to process personal data for another controller pursuant to a contract, empowerment, authorization, or legal regulation,

- g) Employee is a person in an employment or similar relationship with the Employer; for the purposes of personal data protection, an Employee means also another person who performs work for the Employer,
- h) scope of personal data processing means determining the processing method, period of retaining, means of processing, definition of recipient categories and reasons for processing. The determination of the scope of personal data processing also includes the definition of the legal grounds for processing, and for personal data obtained from a Data Subject, identification whether the collecting of personal data is based on a legal or contractual requirement or a requirement for the personal data to be part of a contract, as well as advice to the Data Subject regarding consequences of failure to provide personal data,
- i) Key means the key to the personal data protection, which is a tool for defining the purpose and scope of personal data processing, available at www.oou.cloud,
- j) Office means the Office for Personal Data Protection.

PART TWO

RESPONSIBILITIES OF PERSONS IN CHARGE OF PERSONAL DATA PROTECTION

Art. 3

Guarantor of Personal Data Processing

(1) For the purpose of ensuring the protection of personal data and their processing in compliance with the GDPR and Act on Personal Data Protection, the guarantors of personal data processing are appointed for individual cases or areas of processing (hereinafter referred to as the “Guarantor”). The Guarantors for individual processing purposes are appointed by the Rector; the Rector’s Office keeps the list of Guarantors and their authorizations.

(2) Guarantor

- a) is responsible for observing principles, rules and procedures in the personal data processing within the case/area/activity entrusted to him/her,
- b) after prior consultation with the data protection officer reports a personal data breach to the Data Subject (Art. 34 GDPR).

(3) The Guarantor is responsible for the above activities since the date of appointment until the end of the activities, including the safe archiving of data.

Art. 4

Employees

(1) Employees are entitled to become acquainted with personal data only to the extent that is necessary for the performance of their work and shall be responsible for the processing of such personal data.

(2) Employees are obliged to become acquainted with the determined purpose and scope of such personal data, which they encounter in the course of their work, through documents available at http://www.oou.cloud/katalog/sady?u_id=72.

(3) Within the responsibility of employees for the processing of personal data, employees must not exceed the scope of processed personal data that was determined by the Controller.

(4) Employees are obliged to maintain secrecy concerning personal data and security measures, whose disclosure would endanger personal data security. The obligation of confidentiality shall survive the termination of employment or of work performance.

(5) Employees are obliged to process personal data only in methods and scope determined by the Controller.

(6) Employees are obliged not to enable disclosure of personal data to unauthorized persons. For that purpose, Employees shall observe in particular the “clean desk” policy, i.e. shall not leave documents containing personal data on the desk and shall switch off their computers.

(7) Employees are obliged to inform the Guarantor and data protection officer of a potential data breach and its extent without undue delay.

PART THREE

DATA PROTECTION OFFICER

Art. 5

Position of Data Protection Officer

(1) The data protection officer at JAMU is JUDr. MgA. Michal Šalomoun, Ph.D., Attorney-at-Law, Bráfova tř. 52, 674 01 Třebíč, tel.: 776048017, e-mail: advokacie@oou.cz.

(2) The data protection officer is involved in all processes and issues associated with the protection and processing of personal data at the Employer.

(3) The data protection officer is not assigned any particular instructions by the Employer, concerning the fulfillment of the officer's duties.

(4) The data protection officer is bound by the obligation of confidentiality in connection with the performance of his/her tasks.

Art. 6

Tasks of Data Protection Officer

(1) The data protection officer in particular performs the following tasks:

- k) provision of information and consultancy to Employees and Guarantors who process personal data, concerning their duties in the area of personal data protection,
- l) supervision over the personal data protection and processing in practice,
- m) provision of consultancy and expert assistance upon request in terms of assessing the impact on the personal data protection, and monitoring its compliance under Art. 35 GDPR,
- n) after prior consultation with the Guarantors, reporting a personal data breach to the supervisory authority (Art. 33 GDPR),
- o) cooperation and communication with the supervisory authority,
- p) contact point for the supervisory authority in issues concerning the personal data processing including prior consultation under Art. 36 GDPR,
- q) accepting proposals from Employees for initiation of a new or change to the hitherto purpose of personal data processing and expressing opinions of such proposals,
- r) communication with Data Subjects who may address him/her is all issues associated with the protection and processing of their personal data and with exercise of their rights under the GDPR and this Directive.

(3) In performing his/her tasks, the data protection officer takes due account of the risk involved in the processing activities and at the same time, of the nature, scope, context and purposes of processing.

(4) In case the data protection officer learns of an impending breach of data protection rules or if such breach is detected, he/she shall notify the Guarantor and give written recommendation of action to remove the defective or risky condition. The Guarantor is obliged to discuss the situation with the data protection officer within a reasonable period, and if he/she identifies with the officer's findings, to refrain from further defective or hazardous steps. The Guarantor is also obliged to adopt any measures to prevent the situation from occurring in the future. If the Guarantor disagrees with the data protection officer's recommendation, he/she shall give written justification of the criticized conduct and state reasons why he/she thinks the breach of rules mentioned in the first sentence of this paragraph has not occurred and is not impending. In such case, the data protection officer shall report the facts to the Rector and shall refer all the relevant documents to the Rector.

PART FOUR

PRINCIPLES OF PERSONAL DATA PROTECTION AND THEIR IMPLEMENTATION

Art. 7

Personal Data Processing Principles

The principles relating to the processing of personal data are set out in Art. 5 GDPR. Under that Article, the 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 unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Art. 8

Transparency

(1) The Controller shall process the personal data in a transparent manner so that anyone may become acquainted with the personal data processing.

(2) In order to comply with the transparency principle, the Controller shall publish any and all information on personal data processing on the Internet, classified according to individual processing purposes. Such information is available at http://www.oou.cloud/katalog/sady?u_id=72 in the section Database of information on personal data processing.

Art. 9

Determination of Purpose and Scope of Personal Data Processing

The Controller shall determine the purpose and scope of personal data processing by means of the Key.

Art. 10

Fulfillment of Controller's and Processor's Duties

(1) The duties of the Controller and the Processor shall be fulfilled by the Guarantors unless stipulated otherwise herein below.

(2) The Employer shall be represented by the Rector or the data protection officer before the Office.

(3) Documents and information for any negotiations with the Office shall be prepared by the Guarantor for the Rector.

Art. 11

Personal Data Security

(1) Documents and mobile/external/portable data carriers held by the Employer and containing personal data shall be stored solely in lockers at the Employer's workplaces or, where appropriate, in other secure places determined by the nature of the relevant processing, or secured through encryption.

(2) Computers and other devices on which data containing personal data protected under this Directive are stored must be secured from free access by unauthorized persons, typically by passwords, encryption or locking. Persons in charge are not allowed to leave the computer without logging out, to enable access to unauthorized persons and must protect the secrecy of the credentials.

(3) In the event that a Guarantor or an Employee finds out or suspects that a data breach occurred, he/she shall promptly report it to the data protection officer and the Guarantor in charge.

PART FIVE

EXERCISE OF DATA SUBJECTS' RIGHTS

Art. 12

Information Provided to Data Subjects upon Request

(1) Under Art. 12 GDPR, the Employer in the position of the Controller shall provide any information referred to in Art. 13 and 14 and any communication under Art. 15 to 22 and 34 GDPR relating to processing. The information is also provided electronically at http://www.oou.cloud/katalog/sady?u_id=72.

(2) Data Subjects may address the data protection officer in all issues associated with the protection and processing of their personal data and with exercise of their rights.

(3) The Guarantor or the data protection officer shall comply with the Data Subject's right by advising him/her to visit http://www.oou.cloud/katalog/sady?u_id=72, where the information is classified according to processing purposes.

(4) If the Data Subject insists on another manner of obtaining information, he/she shall be provided the information in PDF documents kept by the data protection officer.

(5) The Data Subjects shall be subsequently informed in the following manner: the Employees who are in touch with Data Subjects via e-mail or written communication shall include the below text into the first e-mail or document addressed to the Data Subject: Informing the Data Subject on the processing of personal data: Information about personal data processing are published by JAMU as the Controller at http://www.oou.cloud/katalog/sady?u_id=72, where information about processing may be searched according to the purpose of processing, or, as the case may be, another text which shall specify the content of the processing purpose and information related to such processing of personal data, stated at http://www.oou.cloud/katalog/sady?u_id=72.

Art. 13

Other Rights of Data Subjects

(1) The Data Subject shall have the right to:

- g) access the personal data under Art. 15 GDPR,
- h) rectification under Art. 16 and 19 GDPR,
- i) erasure under Art. 17 and 19 GDPR,
- j) restriction of processing under Art. 18 and 19 GDPR,
- k) data portability under Art. 20 GDPR,
- l) raise objection, and automated individual decision-making under Art. 21 and 22 GDPR.

(5) Other rights shall be complied with by the Guarantor with the assistance of the data protection officer.

Art. 14

Final Provisions

(1) The protection of personal data which has so far been carried out by the Employer shall be brought into conformity with this Directive within one month of the effective date hereof.

(2) This Directive becomes effective on 1 January 2019.

prof. Mgr. Petr Oslzlý
Rector

Contents

PART ONE	GENERAL PROVISIONS
Art. 1	Subject and Purpose
Art. 2	Definition of Certain Terms
PART TWO	RESPONSIBILITIES OF PERSONS IN CHARGE OF PERSONAL DATA PROTECTION
Art. 3	Guarantor of Personal Data Processing
Art. 4	Employees
PART THREE	DATA PROTECTION OFFICER
Art. 5	Position of Data Protection Officer
Art. 6	Tasks of Data Protection Officer
PART FOUR	PRINCIPLES OF PERSONAL DATA PROTECTION AND THEIR IMPLEMENTATION
Art. 7	Personal Data Processing Principles
Art. 8	Transparency
Art. 9	Determination of Purpose and Scope of Personal Data Processing
Art. 10	Fulfillment of Controller's and Processor's Duties
Art. 11	Personal Data Security
PART FIVE	EXERCISE OF DATA SUBJECTS' RIGHTS
Art. 12	Information Provided to Data Subjects upon Request
Art. 13	Other Rights of Data Subjects
Art. 14	Final Provisions