doc. Jan Hančil
rektor / rector

Ref. 900/18/00061
PID 0310831

Prague, 28 February 2018

RECTOR'S DECREE No. 5/2018

Protection and Processing of Personal Data

The Decree takes effect on 25 May 2018.

AKADEMIE MÚZICKÝCH UMĚNÍ V PRAZE
ACADEMY OF PERFORMING ARTS IN PRAGUE
DAMU FAMU HAMU

Malostranské náměstí 12
118 00 Praha 1
Czech Republic
www.amu.cz

T: +420 234 244 501
E: jan.hancil@amu.cz
IČ: 61384984, DIČ: CZ61384984
ID datové schránky: ikwj9fx

Protection and Processing of Personal Data

(Wording effective from 25 May 2018)

Under Section 10(1) of Act No. 111/1998 on universities and on amending certain other acts (the University Act), as amended (the "Act"), I hereby issue the present Decree:

Part one – Principal provisions

Article 1 – Subject matter

(1) This Decree lays down the principles and rules for the processing of personal data at the Academy of Performing Arts in Prague ("AMU"), defines the responsibility of the persons in charge of protecting personal data at AMU, and defines the rights and obligations of the employees, students and/or other natural persons and legal entities involved in activities connected with the processing of such data.

(2) The subject matter of this Decree is the processing of personal data by AMU employees and students during the observance of their professional or study obligations, and/or by other natural persons and legal entities that process personal data under a contract with AMU.

(3) This Decree is based on the Regulation of the European Parliament and of the Council (EU) No. 2016/679 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 "GDPR") and on Act No. 101/2000 on the protection of personal data and amending certain acts, as amended (the "Act"), and it complements and develops certain provisions thereof for application at AMU and defines the organisational solution for their application at AMU.

(4) This Decree does not restrict the validity of Act No. 499/2004 on archiving and file service, in particular with regard to the storage of both analogue and digital documents, the validity of periods for shredding documents, and discharging certain documents (information) as part of the shredding procedure.

Article 2 – Interpretation of certain related terms

(1) "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. Data referred to as "sensitive" in GDPR requires special protection;

(2) "personal data processing" means 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;

"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;

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

(4) "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;

(5) "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;

(6) "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;

(7) "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;

(8) "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;

(9) "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;

(10) "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;

(11) "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;

(12) "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;

(13) "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;

(14) the definitions of other terms used in handling and protecting personal data are provided in Articles 4 and 10 GDPR (sensitive data), and/or within the body of and/or the attachments to this Decree where appropriate.

Part two – Responsibility of persons in charge of personal data protection

Article 3 – Position of AMU

AMU is the entity responsible for the processing of personal data specified in clause 1(2). Depending on specific cases, AMU may act as the controller and/or as the processor. In order to protect personal data as required by GDPR and the Act, part two of this Decree defines the persons involved in meeting the above purpose.

Article 4 – Responsibility

(1) The position of the Rector is defined by law, the Statute of AMU, and other internal policies of AMU. The Rector acts as AMU's governing body, responsible for the observance of the principles, rules and procedures in processing personal data within and outside AMU in the cases covered by AMU on a central level and where power has not been delegated to other persons specified in this part.

(2) The Bursar and the Heads of the individual sections at AMU answer to the Rector of AMU with regard to the observance of the principles, rules and procedures in processing personal data in the field of their competence as specified in Article 12 of the Statute of AMU.

(3) The persons specified in clause (2) are responsible for the observance of the principles, rules and procedures (specified in this Decree, GDPR and other relevant legal regulations of general application) in the processing of personal data taking place in the cases/areas/activities entrusted to them. They are responsible for said activities from the date of their appointment until the end of the activity, including ensuring safe archiving of the data.

(4) Persons specified in clause (2) shall assess the effect of the intended processing operations on personal data protection under Article 35 GDPR. To that end, they shall request an assessment from the data protection officer.

Article 5 – Other authorised persons

(1) Persons who may come in contact with personal data:

a) persons in charge of collecting and deleting personal data depending on the characterisation of processing under Article 13;

b) persons senior to the persons specified under indent a) above in organisational or methodological terms;

c) persons in charge of organisational, functional, and technical management of personal data processing (officers in individual sections, system and network administrators, etc);
d) other persons authorised to use such personal data to deliver on their work tasks depending on the characterisation of processing under Article 13.

(2) Persons may be recruited or assigned to positions involving the authorisation under clause 1 provided that they previously demonstrably familiarise themselves with this Decree, GDPR and other relevant legal regulations of general application.

(3) Persons specified in clause 1 are obligated to process personal data exclusively to the extent of the requirements for implementation/type solutions of data processing under Article 4.

(4) Persons specified in clause 1 are obligated to keep confidential any personal data and security measures whose publication would compromise personal data security. The non-disclosure obligation shall survive the end of employment, study, or provision of any relevant work and is defined in a separate document.

Article 6 – Graduation and other papers by students

Should a student's graduation paper (bachelor's, master's, and/or dissertation thesis) involve processing personal data, the thesis supervisor shall instruct the student as to the obligations under GDPR and this Decree and take any other steps required under the Decree. Generally, this duty also applies to other cases where students work on projects or other activities as part of their duties that involve personal data processing. Further details may be laid down by a special measure of AMU.

Part three – Data protection officer

Article 7 – Appointment of the data protection officer

AMU's data protection officer (the "data protection officer") is appointed by the Rector based on their professional qualities, including but not limited to their expert knowledge of law and practice in the field of personal data protection, and their ability to fulfil tasks specified in Article 11. The Rector may also recall the data protection officer. The status, activities, and power of the data protection officer is the subject matter of a separate Rector's Decree.

Article 8 – Position of the data protection officer

(1) The data position officer is either an AMU employee or a natural person or legal entity that provides the relevant services to AMU under a contract.

(2) The data protection officer answers directly to the Rector.

(3) The data protection officer is involved in all the processes and affairs related to the protection and processing of personal data at AMU.

(4) AMU encourages the data protection officer to maintain their professional knowledge and allows them access to personal data, processing operations and all the resources required for delivering on tasks specified in clause 9.

(5) AMU does not give the data protection officer any specific instructions in connection with fulfilling their obligations as the data protection officer. However, the Rector may entrust the data protection officer with fulfilling tasks and obligations. None of such tasks or obligations should result in a conflict of interests with the position of a data protection officer.

(6) The data protection officer is bound by a non-disclosure obligation in connection with their tasks. The non-disclosure obligation shall survive the end of employment or contract with AMU.

(7) Information about the data protection officer, including contact information, is provided in the public section of AMU's website.

Article 9 – Tasks of the data protection officer

(1) The data protection officer fulfils, without limitation, the following tasks:

a) to inform and advise AMU's employees and/or students who process personal data of their obligations pursuant to this Decree, GDPR and other legal regulations of general application in the field of personal data protection;

b) to monitor compliance with this Decree, GDPR, other legal regulations of general application in the field of personal data protection and AMU's concepts for personal data protection, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations;

c) oversee the protection and processing of personal data;

d) to provide advice and technical aid where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 GDPR;

e) following prior consultation with persons specified in Articles 4 and 5, to report any cases of personal data breach to the supervisory authority (Article 33 GDPR) and to report any cases of personal data breach to the data subject (Article 34 GDPR).

f) to work and communicate with the supervisory authority;

g) to act as a point of contact for the supervisory authority in matters related to processing personal data, including prior consultation under Article 36 GDPR, and, as the case may be, to organise consultations in any other matters;

h) to receive suggestions for starting new processing or changing the existing processing of personal data from AMU's employees and takes a position on the suggestions;

i) to communicate with data subjects who may contact them with regard to any matters related to the processing of their personal data and exercising their rights under this Decree and GDPR;

j) to fulfil other tasks arising for the position from GDPR, this Decree, the Act or legal regulations of general applications, or arising from this Decree and other AMU policies.

(2) The data protection officer oversees the functioning of the AMU registry for personal data processing specified in Article 11.

(3) The data protection officer fulfils their obligations with due regard to the risk related with processing activities and to the nature, scope, context, and purpose of processing.

Article 10 – Data protection officer's competence at AMU

(1) If the data protection officer learns that a threat that the personal data protection rules arising from GDPR, the Act or this Decree can be or have been breached, the data protection officer shall notify the responsible person under clause 4(2) and recommend rectifying the flaw or risk in writing. The responsible person shall discuss the situation with the data protection officer within an adequate period of time and, if the person agrees with the data officer's findings, shall refrain from

any further defective or risk actions. The person shall also adopt all measures to prevent the situation from repeating. If the person disagrees with the data protection officer's recommendation, the person shall justify the actions pointed out in writing to the data protection officer and give reasons why they do not believe there is a threat of breach or a breach of the rules specified in the first sentence. In such a case, the data protection officer shall report this to the Rector of AMU and give the Rector all the documentation.

(2) The data protection officer shall submit a suggestion for adopting general or individual measures in personal data protection to persons specified in Articles 4 and 5 every time when:
   a) they detect a threat of breaching or a breach of rules based on their conclusions as per clause 1 above;
   b) this is fitting in connection with generalising the practice in personal data protection.

(3) The provisions of clauses 1 and 2 are not to the detriment of the data protection officer's obligation to communicate a personal data breach to the supervisory authority and the data subject following a prior consultation with the persons specified in Articles 4 and 5 under clause 9(1)(e).

Part four – Registry of personal data processing at AMU

Article 11 – Registration and filing system for personal data processing

(1) An electronic registry of the personal data processing activities is set up with a view to tracking personal data at AMU (the "registry"). The AMU Computer Centre ("AMU CC") is entrusted with running the registry. The Head of AMU CC is responsible for the operation of the registry.

(2) If personal data are processed by the components of the AMU Information System ("AMU IS") or in relation to it, the records of the processing activities shall be tracked in AMU IS. The AMU CC is in charge of the operation. The Head of AMU CC is responsible for the activity. In the event of doubt as to whether or not processing is covered by clause 2, the Vice-Rector in charge shall decide.

(3) Sections of AMU that process or wish to process personal data protected by this decree and/or wish to change the existing method of processing personal data shall notify this to the data protection officer through the registry.

(4) The notification under clause 3 must contain a full description of the processing of the personal data concerned. The scope shall be defined by an AMU measure.

(5) The proponent has the right to start new/change the existing processing of personal data only after having received an official position from the data protection officer further to the notification. If the position is negative, the matter will be discussed with the persons specified in Articles 4 and 5.

Part five – Principles of processing personal data

Article 12 – Principles of processing personal data

(1) The principles of processing personal data are specified in Chapter II GDPR. In accordance with it, personal data shall 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; processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) Persons specified in Articles 4 and 5 of this Decree are responsible for the observance of the principles under clause 1, and they shall be capable of documenting the observance.

Article 13 – Lawfulness of processing

(1) Under Article 6 GDPR, processing shall be 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 conditions of consent are detailed in Articles 7 and 8 GDPR);
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 in accordance with legal regulations of general application;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller in accordance with legal regulations of general application;
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) Clause 1(f) does not apply to the processing of personal data by AMU in cases where AMU acts as an official authority in matters vested in its power 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 legal regulations of general application, the responsible person 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 AMU;

c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 GDPR;
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 14 – Processing of special categories of personal data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited in cases not covered by clauses 2 and 3.

(2) Exemptions from the prohibition of processing personal data under clause 1 are defined in Article 9 GDPR.

(3) Exemptions from the prohibition in clause 1 include information on:
a) health status in employees' and students' personal records, provided that such data were provided to such records by the data subjects on a voluntary basis and are kept for the data subject's benefit (e.g., they have an influence on admission to study, provision of services to persons with special needs, accommodation in dormitories, or the calculation of tax and/or other statutory levies);
b) membership in trade unions active at AMU mentioned in personal and payroll records of employees, provided that the data were provided to such records by the data subject son a voluntary basis and serve for the payments of membership fees or other levies, including the account carrying of such payments);
c) biometric data enabling direct identification or authentication of data subjects;
d) special categories of personal data processed for project/research purposes.

(4) Data defined in clause 1 may be processed only subject to the express consent of the data subject. The consent shall be given in writing and signed by the data subject, and it must clearly indicate the data it applies to, the purpose, the period, and the party giving the consent. With his or her signature, the data subject also confirms that they have been instructed about their rights. The authorised persons who are tasked with entering and deleting said data depending on the description of the relevant data processing under Article 6 must be capable of proving the existence of such consent throughout the entire period of processing such data.

(5) Data processing under clause 3(c) may be used only if an option exists for achieving the same purpose using other means of identification or authentication not dependent on biometric data and if the data subject can choose between them.

(6) The processing of personal data which does not require data subject identification is covered in Article 11 GDPR.

Article 15 – Implementing regulations

Implementing regulations relevant for this Decree shall be issued.

Part six – Data subject

Article 16 – Information to be provided to the data subject

(1) AMU as the controller shall give the data subject, in accordance with Article 12 GDPR, all information specified in Articles 13 and 14 GDPR in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and shall make any and all communications under Articles 15 to 22 and 34 GDPR on processing. The information is provided electronically on the AMU website and in AMU's information systems.

(2) Data subjects may approach the data protection officer with all issues related to the processing of their personal data and the exercise of their rights under this Decree and GDPR.

Article 17 – Rights of the data subject

The right of the data subject to:

a) access to personal data is laid down in Article 15 GDPR;
b) rectification and erasure is laid down in Articles 16 and 19 GDPR;
c) erasure is laid down in Articles 17 and 19 GDPR;
d) restriction of processing erasure is laid down in Articles 18 and 19 GDPR;
e) data portability erasure is laid down in Article 20 GDPR;
f) right to object and automated individual decision-making is laid down in Articles 21 and 22 GDPR.

Part seven – Disclosure and security of personal data, and provision to third parties

Article 18 – Disclosure of personal data

(1) Disclosure of personal data means making it accessible to unspecified persons or groups of persons, including but not limited using mass media, by other public notification, or as part of a public list (e.g., in a public section of AMU's website).

(2) Personal data protected under this Decree may be disclosed to the maximum extent of:

a) first name;
b) surname;
c) degrees;
d) user name (login) in the AMU network;
e) personal number;
f) photograph;
g) job position at AMU;
h) position within AMU's organisational structure;
i) positions held at AMU;
j) contact details relating to AMU (worksite addresses, telephone and facsimile numbers, e-mail addresses);
k) CV;
l) course of academic qualification;
m) involvement in the various forms of AMU's creative activity;
n) information on publications released;
o) instruction provided at AMU;
p) personal academic websites (i.e., websites of AMU employees and students connected with their academic activities and/or study at AMU);

q) any other data that a data subject discloses about him or herself.

The data subject has the right to choose the specific scope of the information to be disclosed under indents f), k), and p), or not to disclose such data at all.

(3) The data specified in clause 2 can be disclosed only if pertaining to data subjects who:
   a) are AMU employees;
   b) are AMU employees or students and are currently active on AMU's self-government academic or advisory bodies within AMU;

(4) For academic officials and heads of AMU sections, the disclosure of personal data shall be addressed on an individual basis.

(5) For academic officials and persons currently active on AMU's self-government academic or advisory bodies who are not AMU employees, the disclosure of personal data shall be addressed on an individual basis.

Article 19 – Provision of personal data to third parties

(1) Provision of personal data to third parties outside AMU shall be governed by this Decree, GDPR and legal regulations of general application.

(2) The data protection officer must be informed about any provision of personal data to a third party outside AMU in writing in advance, including the scope of the data provided, the purpose of the disclosure and the identification of the third party.

(3) The relevant persons specified in Articles 4 and 5 are responsible for the compliance with the correct procedure in the provision of personal data to third parties outside AMU in accordance with this Decree, GDPR, and legal regulations of general application.

Article 20 – Security of personal data

(1) Written documents and mobile/external/portable technical media for information that AMU owns and that contain personal data protected under this Decree shall be kept only in lockable cabinets at AMU worksites or, as the case may be, in other secure places determined by the nature of processing of the data under Article 12, or secured by encryption.

(2) Where personal data related immediately to activities pursued at AMU (e.g., attendance sheets, reply forms, tests, note pads, presence lists) is processed, their security shall follow the usual procedures to prevent the risk of personal data misuse. Other obligations laid down in this Article shall apply to the processing of such personal data only to the extent that this is adequate to their nature and the circumstances of usual processing.

(3) Computers and other equipment where data containing personal data protected under this Decree are stored shall be secured from free access of unauthorised persons, as a rule using access passwords, encryption, or locking.

(4) Any copies of personal data protected under this Decree shall be made using information media observing the operating rules defined for the various methods of personal data processing and kept in lockable cabinets at AMU worksites or, as the case may be, in other secure places determined by the nature of processing of the data under Article 12, or secured by encryption. The copies shall always be stored in a different room from the original data.

(5) If an authorised person or AMU employee finds out or suspects that personal data breach could occur or occurred, they shall report this promptly to the data protection officer and the relevant persons specified in Articles 4 and 5.

(6) The data protection officer shall notify any cases of personal data breach to the supervisory authority (Article 33 GDPR) and to the data subject (Article 34 GDPR) following a prior consultation with the persons specified in Articles 4 and 5.

Part eight – Final provisions

Article 21 – Final provisions

(1) The data protection officer is in charge of overseeing the compliance with this Decree.

(2) This Decree becomes valid on the day of signing.

Assoc. Prof. Jan Hančil
Rector