Approved at a meeting of the Senate
of the Art Academy of Latvia on
1st April 2020

Art Academy of Latvia's
Internal Data Protection Regulations

The regulations prescribe the Art Academy of Latvia's personal data processing and protection in accordance with Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter – the General Data Protection Regulation).

1. Explanation of Terms Used

1.1. Data subject – a natural person who can be identified directly or indirectly;
1.2. Consent of the data subject – freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him;
1.3. Personal data – any information relating to an identified or identifiable natural person;
1.4. Special category personal data – personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as providing information about a person's genetic or biometric data, health, sex life, or sexual orientation;
1.5. Processing - 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;
1.6. Restriction of processing – the marking of stored personal data with the aim of limiting their processing in the future;
1.7. Controller – Art Academy of Latvia;
1.8. Controller's personal data user – the controller's employee or a person employed on the basis of an outsourcing contract under the controller's direction;
1.9. Processor (personal data operator) – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
1.10. Representative – a legal or natural person, established in the Union and designated by the controller or processor in writing and who represents the controller or processor with regard to their respective obligations;
1.11. Recipient – a natural or legal person, public authority, agency or another body, to which the personal data are disclosed - whether a third party or not. 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;

1.12. Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who are authorised to process personal data under the direct authority of the controller or processor;

1.13. Personal data breach – 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.

2. General Issues

2.1. The processing of personal data is undertaken at the controller's premises, which are located at the following addresses –1) at Kalpaka bulvāris 13 in Rīga, 2) at Avotu Street 36 in Rīga, and 3) at Baznīcas Street 34A in Rēzekne.

2.2. The regulations are binding on all AAL employees and students, as well as other legal or natural persons, if the contract between the AAL and these other legal or natural persons has a reference to these Regulations or the AAL's internal laws and regulations, and are applicable to all personal data which relate to the identified or identifiable natural person,

3. Information Classification

3.1. Information classification levels:

3.1.1. secret – highest level. The disclosure or theft of such information may cause significant or sustained losses and seriously damage the good name of the controller. The greatest care must be taken in working with such information, and this information may only be disclosed in cases of extreme necessity.

3.1.2. restricted access – information which is provided for everyday work and which is provided only to a designated group of employees. The disclosure or theft of such information may cause internal or external inconvenience to the controller. Access to such information is assigned only to authorized employees.

3.1.3. unclassified – information which is already known in the community, which is freely distributed, or which is available to all the controller's employees and other third parties. The disclosure or theft of such information does not affect the work of the controller.

3.2. Data, which is used in processing personal data, can be classified as restricted access information, to which only authorized employees have the right of access and to perform its processing.

4. Technical Resources, with which Personal Data Processing is Performed

4.1. The user performs the processing of the data manually (in paper form), in full or partly with automatized measures (electronically) or mixed in both forms.

4.2. Writing paper, folders, locking or open shelving etc., are used in performing the processing of personal data manually.

4.3. The following technical resources are used in performing the processing of personal data fully or partly with automatized measures (electronically):

4.3.1. Computers (table, laptop or tablet);

4.3.2. Servers;

4.3.3. Computer programs – including the MS Windows operating system.

4.4. The regulations on the use of technical resources are prescribed in the Regulations on the Usage of Information Systems.

5. Password Construction and Usage

5.1. Information system protection is ensured by a computer password, which must conform to the following requirements:

5.1.1. the minimum length of the password must be at least 8 symbols;

5.1.2. the maximum period for changing a password must not exceed 60 days;

5.1.3. the password's construction must be complicated, using combinations of letters, numbers and special characters (like, for example !@#$%^*()_+);

5.1.4. none of the 3 (three) previous passwords can be reused.

5.2. A user must not divulge their password to other employees or any other third persons.

5.3. A user must not write their password down on paper, unless this document is kept in a safe or in another place with restricted access to other persons.

5.4. If a user has suspicions that their password has been discovered by any other person, the employee has an obligation to change this password as soon as possible.

6. Personal Data Processing Principles

6.1. A user observes the following principles in processing personal data:

7.1.2. data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

7.1.3. data shall be collected for specified, explicit and legitimate purposes;

7.1.4. data, which has been collected for a specific purpose may only be processed for this purpose – if it is necessary to process the data for a different purpose, then the consent of the data subject must be obtained;

7.1.5. the data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

7.1.6. the data are accurate and, where necessary, kept up to date;

7.1.7. the data are 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;

7.1.8. the data are 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;

7.1.9. the data are processed only by those persons who require them for performing their direct functions;

7.1.10. the data must be stored at the end of the work day, so that they are not freely accessible to other persons;

7.1.11. the data are processed, carrying out appropriate technical and organizational measures, including pseudonymisation and enciphering in prescribed situations.

8. Legal Basis for the Processing of Personal Data

8.1. A user has the right to perform processing of personal data, if at least one of the following mentioned grounds applies:

8.1.1. The consent of the data subject;

8.1.2. Performance of a contractual obligation;

8.1.3. Performance of a legal obligation;

8.1.4. The vital interests of the data subject or of another natural person;

8.1.5. Tasks carried out in the public interest or in the exercise of official authority;

8.1.6. For the purposes of the legitimate interests pursued by the controller or by a third party, balancing these with the interests of the data subject.

8.2. A user is forbidden from performing the processing of special category data, unless one of the following mentioned grounds applies:

8.2.1. the consent of the data subject;

8.2.2. the carrying out of obligations prescribed in acts and regulations in the field of employment, social security and social protection law;

8.2.3. the protection of the vital interests of the data subject or of another natural person, if the data subject is physically or legally unable to give their consent;

8.2.4. the processing is required about its members by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;

8.2.5. the processing relates to personal data which are manifestly made public by the data subject;

8.2.6. the processing is necessary for the establishment, exercise or defence of legal claims;

8.2.7. the processing is necessary for reasons of substantial public interest;

8.2.8. the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

8.2.9. the processing is necessary for reasons of public interest in the area of public health;

8.2.10. the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

8.3. The user provides the data subject with all necessary information about the data subject's personal data processing and ensures communication with regard to the processing.

9. Consent of the Data Subject

9.1. A user obtains the consent of the data subject as a clearly affirmative action, which means a freely given, specific, informed and unambiguous indication of the data subject's consent to the processing of personal data relating to him, for example, by a written, including electronic, or verbal declaration.

9.2. A user must obtain the explicit consent of the data subject for the processing of special category personal data.

9.3. If the processing is based on consent, the controller or its authorised employee, namely, the user, must be able to unambiguously indicate that the data subject has agreed to the processing of his personal data.

9.4. The user informs the data subject, prior to the data processing, about their rights to withdraw their consent at any time and the fact that the withdrawal of consent does not affect the lawfulness of the processing which was based on the consent prior its withdrawal.

10. Actions in cases of a personal data protection breach or incident

10.1. The user has an obligation to promptly notify the responsible person about any personal data processing breach or incident, no later than 48 hours' time from the moment, when the breach has become known, including:

10.1.1. if any kind of threat to technical resources (an interruption to the power supply, the entry of liquid or foreign bodies, damage as a result of a physical shock, the impact of fire or floods etc.) is established;

10.1.2. if any kind of threat to information resources (third parties have come to know the password for access, unauthorized access has been established, interruptions to operations have been established etc.) is established.

11. Procedure for the Storage and Destruction of Data Carriers

11.1. The procedure for the storage and destruction of data carriers is prescribed by the Archives Law and the Cabinet of Ministers Regulations issued based on it.

11.2. Documents in paper form are to be destroyed using paper shredding equipment, while electronic documents – irreversibly erased using the corresponding software, after the end of their period of storage.

12. A User's Rights, Obligations and Responsibility

12.1. Users confirm by their signature that they are responsible for the observation of these regulations (Appendix "Statement on the Observation of the Requirements of the Academy of Latvia's Internal Data Protection Regulations").

12.2. It is the obligation of users to become familiar with the Regulations and to observe these in their everyday work.

12.3. A user must not allow other persons access to personal data unless it is required for the direct discharge of their work obligations and authorization has been provided by the Controller.

12.4. A user is not allowed to copy documents containing personal data, files on external data carriers (diskettes, USB cards and/or compact disks), unless it is required for the

direct discharge of their work obligations and/or authorization has been provided by the Controller.

12.5. On finishing work, a user has an obligation to place documents containing personal data in lockable cupboards and to turn off their computer completely, but if the user leaves their computer for a relatively short time, then the user must use a screensaver with a password. The door should be locked on leaving the workspace, and at the end of the working day it should be connected to security.

12.6. On the request of a data subject, coordinating this with the responsible person, users are obliged to provide them with all the information that has been collected on the corresponding data subject, at no cost, within a month of the day of the submission of the request.

12.7. At the request of a responsible person, a user is to correct or add to the incorrect personal data of the data subject without unjustified delay.

12.8. The user has an obligation to notify the responsible person about the data processing and to point out the erasure of personal data, in cases where:

12.8.1. personal data is no longer necessary in connection with the purposes for which they were collected or otherwise processed;

12.8.2. a data subject withdraws their consent on the basis of which the processing was performed, and if there is no other legal basis for the processing;

12.8.3. a data subject objects to the processing in accordance with Article 21 (1) of the General Data Protection Regulation, and the processing has no other more important legitimate basis, or the data subject also objects to the processing in accordance with Article 21 (2) of the Regulation;

12.8.4. the personal data has been processed illegally;

12.8.5. the personal data must be erased to ensure that a legal obligation is being complied with, which has been prescribed in the legislation of the Union or a member country, which are applicable to the controller;

12.8.6. personal data has been collected in accordance with the provision of information society services, as mentioned in Article 8 (1) of the General Data Protection Regulation.

12.9. A user has an obligation to provide notification of a restriction on the processing of personal data, on the existence of the following criteria:

12.9.1. If a data subject challenges the accuracy of personal data – for the period in which the controller can check the accuracy of the personal data;

12.9.2. If the processing is illegal, and the data subject objects to the erasure of the personal data and requests a restriction on the use of the data instead;

12.9.3. If the personal data is no longer required for processing by the controller, but they are required by the data subject to institute, pursue or protect their legal entitlements;

12.9.4. If a data subject has objected to the processing in accordance with Article 21 (1) of the General Data Protection Regulation, for the period until it has been checked, or the controller's legitimate reasons are not more important than the legitimate interests of the data subject.

12.10. A user is required to provide notification about data processing to the responsible person or to the data protection specialist, if such has been appointed.

12.11. A user, on request, provides a data subject personal data in relation to themselves, which the data subject has provided to the controller's employee, in a structured, widely used, machine readable format.

12.12. A user is responsible for computer equipment which has been provided at their disposal, and the user is also responsible for the activities which are performed with the computer equipment provided to it.

12.13. A user also undertakes to maintain the confidentiality of information after the legal termination of the work relationship.