Approved by Supervisory Board of Foundation Euroopa Kool on 18 June 2019

Tallinn European School

PERSONAL DATA PROCESSING PROCEDURE OF TALLINN EUROPEAN SCHOOL

1. GENERAL PRINCIPLES

1.1. This personal data processing procedure (hereinafter the Procedure) provides the principles of personal data processing, rights of the data subject and obligations of **Tallinn European School** (hereinafter the European School). The legal entity and owner of the European School is Foundation Euroopa Kool (90014537, Tehnika 18, 10149 Tallinn) who is the data controller for all personal data processed in relation to the activities of the European School. The direct contact of your data controller for all communication relating to personal data is the following: **Iris.maeker@est.edu.ee (data protection officer)**.

1.2. The processing of the data of the visitors of the webpage of the European School is mainly regulated with the privacy policy published on the website. In case of aspects not regulated therein, this Procedure applies.

1.3. The European School processes personal data based on the General Data Protection Regulation (GDPR) (EU) 2016/679[1], other applicable legal acts, and the following principles:

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

1.3.2. the data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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

1.3.4. the data is accurate and, where necessary, kept up to date;

1.3.5. the data is 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;

1.3.6. the data is 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.

1.4. 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.

1.5. 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 are considered special categories of personal data, that are subjected to a higher level of protection.

1.6. The record of processing activities under the responsibility of the European School is maintained by Foundation Euroopa Kool. The record includes information about the activities of the European School, their purposes, the types of personal data processed, the categories of data subjects, time limits of erasure (where possible), general description of the technical and organisational security measures (where possible), and other information required by the applicable law.

2. PURPOSES AND BASES OF PROCESSING PERSONAL DATA

2.1. The European School processes personal data only for legitimate purposes and only in the extent that is required for realisation of the statutory activities. The legal basis for majority of the processing is either a) performance of contracts, b) taking steps to conclude a contract, c) obligations deriving from the law, or d) legitimate interest.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

2.2. The purposes for which the European School processes personal data are listed in the record of processing activities. Such data can be divided under two main categories: provision of educational services under the European Baccalaureate curriculum and offering extracurricular activities.

3. PERSONS WHOSE DATA IS BEING PROCESSED

3.1. The record of processing activities of the European School lists the categories of data subjects, whose data is processed by the European School. The main categories are the following:
  3.1.1. The European School processes the data of its employees (who have an employment agreement) and of the persons offering services under a different type of agreement.
  3.1.2. In the course of providing education services, the European School processes the personal data of the students attending the school, and parents or legal representatives of those students.

4. CATEGORIES OF THE PERSONAL DATA BEING PROCESSED

4.1. The categories of personal data that the European School processes are listed in the record of processing activities. The main categories are the following: names, contact data, ID codes or dates of birth, bank account data, CV data, language skills, academic results/levels.
4.2. In justified cases, the European School processes personal data that falls under special categories (subjected to heightened protection). Such data most often constitutes health data – mostly in cases where the student has special needs, which the school must be informed of, in order to ensure the safety of the student, or to adapt the environment or teaching process.

5. THIRD PERSONS WHO ARE AUTHORIZED TO RECEIVE AND PROCESS PERSONAL DATA

5.1. The categories of third persons that the European School transfers personal data to are listed in the record of processing activities.
5.2. The European School only discloses and/or transfers personal data to third persons, including third persons in foreign countries, if such third persons are entitled to this according to law or other legal acts or (international) agreements, and to the following persons, if necessary and legally permitted:
  5.2.1. health care service providers;
  5.2.2. European school parents` organization(s);
  5.2.3. service providers to the European School (including payment, communication, legal assistance and/or IT service providers);
  5.2.4. the Estonian Education Information System (EHIS);
  5.2.5. the European Schools general educational data system;
  5.2.6. previous and future educational institutions of a student;
  5.2.7. inquiries to (former) employers (as regards of personnel and a parent or legal representative);
  5.2.8. traineeship companies.
5.3. If the data subject has not given the European School a separate permission, the European school discloses and/or transfers personal data of special categories only in cases and for persons provided by law.
5.4. The European School registers the transfer of personal data to third persons according to internal procedure rules.

6. RIGHTS OF THE DATA SUBJECT AND ACCESS TO DATA

6.1. The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, obtain

information about that data (purposes, categories, recipients, storage period, rights that the data subject has, instructions about filing a complaint, sources of the data).

6.2. The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

6.3. The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

6.3.1. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

6.3.2. the data subject withdraws consent;

6.3.3. the data subject objects to the processing (and there are no overriding legitimate grounds for the processing);

6.3.4. the personal data has been unlawfully processed;

6.3.5. the personal data has to be erased for compliance with a legal obligation to which the controller is subject.

6.4. The data subject has the right to obtain from the controller restriction of processing where one of the following applies:

6.4.1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

6.4.2. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

6.4.3. the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims;

6.4.4. the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

6.5. Where processing has been restricted under the previous clause, such personal data is, with the exception of storage, only to be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

6.6. The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit such data to another controller without hindrance from the controller to which the personal data have been provided, if the processing is based on consent or on a contract; and the processing is carried out by automated means.

6.7. If the processing is done based on consent only, then the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

6.8. The data subject has a right to get information about the storage period of his/her personal data. The storage periods of different types of data are regulated with the relevant procedure documents of Foundation Euroopa Kool (*List of Documents of Tallinn European School*). For example, the personal folders of the students are preserved for 50 years, the contracts concluded with students for 10 years as of termination, and the school admission applications are preserved for 5 years.

6.9. The data subject has a right to know if the provision of particular personal data to the European School is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data. For example, the data collected by the European School at the time or before of concluding a schooling contract is necessary for fulfilment of the contract. The contract cannot be properly fulfilled without such data. Also, the data regarding any special needs of the student is also necessary for proper fulfilment of the contract.

7. OBLIGATIONS OF EMPLOYEES AND THE EUROPEAN SCHOOL

7.1. The employee of the European School who processes personal data undertakes:

7.1.1. to process personal data according to the aims and conditions and instructions provided by the applicable legal acts, this Procedure and/or other procedures related to the processing of personal data provided by the employer;

7.1.2. not to disclose the personal data revealed to him/her during the performance of his/her employment duties even after the completion of the tasks related to the processing of personal data or after the termination of the employment relationship;

7.1.3. to participate in personal data protection trainings, if and when they are offered by the employer;

7.1.4. to be familiar with and base his/her work on the laws applicable to data protection (mainly the General Data Protection Regulation);

7.1.5. **to notify the data protection officer of Foundation Euroopa Kool immediately, if the employee notices any adverse incident involving personal data (or possibility thereof). The contact info is the following: iris.maeker@est.edu.ee. When notifying of an in incident or a possibility thereof, the employee should specify as many details as possible, even if they may seem insignificant.**

7.2. The European School undertakes to:

7.2.1. immediately delete or close the personal data not needed for achieving the purposes it was obtained for, if no other legal basis remains for processing it;

7.2.2. ensure that personal data in its possession is correct and updated;

7.2.3. stop any processing (other than maintaining) of any personal data that appears to be incomplete or incorrect, and take immediate measures to complement or amend such data;

7.2.4. maintain incorrect data together with the correct data and note about the time the incorrect data was used;

7.2.5. stop any processing (other than maintaining) of such personal data the validity of which has been disputed until the validity of data or the correct data has been established;

7.2.6. in case of any rectification or erasure of personal data or restriction of processing is carried out by the European School, the European School shall notify each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The European School shall inform the data subject about those recipients if the data subject requests it;

7.2.7. **if a personal data breach is detected, notify the supervisory authority (*Andmekaitse Inspektsioon*) without undue delay (where feasible, not later than 72 hours after becoming aware of the breach). This obligation does not apply in case the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons**. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification must at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.2.8. **When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the European School shall communicate the personal data breach to the data subject without undue delay.** The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of clause 7.2.7 above. The communication to the data subject is not required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

8. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

8.1. The aim of the security measures implemented to protect personal data is to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and service; to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; to ensure a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
8.2. The European School ensures the integrity, availability and resilience of processing systems and service through organisational, physical, and technological security measures (including training the employees on the topic of data protection, security measures of the building (including entry with an entrance card), restrictions to the accessibility to the data systems).
8.3. The principles of document management and IT security are specified in the respective procedures.
8.4. Personal data that is being processed by the European School is mainly on paper as documents or in a digital form on data mediums and server, which can be accessed by using unique usernames and passwords (including in some cases, access only with the Estonian ID card or a special code given by the European School General Office).
8.4.1. The document management system of Foundation Euroopa Kool implements different limitations to authorized access to different groups of employees. It also keeps a log, which allows to determine who and when accessed whish data and what changes were made. The documents containing personal data are protected with limitations to viewing rights, in accordance to the procedures established in Foundation Euroopa Kool.
8.4.2. The personal data kept in other databases are protected with contractual means, personal passwords and the periodical internal review of the granted rights.
8.4.3. The access to servers is limited with usernames and passwords. Personal data copied to portable carriers are encrypted.
8.4.4. Paper documents or transferable data mediums that include personal data are kept in locked metal cupboards or in a safe. Only the possessor of the key of the locked cupboard or safe has the access to delicate personal data.

9. COMPLAINTS

9.1. If the data subject finds that his/her rights are being violated by the European School processing the personal data, the data subject is entitled to turn to the European School with the request to terminate the violation. The contact information of the European School for personal data related complaints is the following: iris.maeker@est.edu.ee (data protection officer). The data protection officer is designated in accordance to the General Data Protection Regulation and the details of the designated person are communicated to the supervisory authority. The data protection officer is independent in their activities and monitors that the personal data is protected in accordance to the applicable legal requirements.
9.2. The data subject is also entitled to lodge a complaint with the Data Protection Inspectorate (*Andmekaitse Inspektsioon*) or with a competent court at any time. The contact info of the Data Protection Inspectorate is the following: Väike-Ameerika 19, Tallinn 10129; +372 627 4135;

info@aki.ee; http://www.aki.ee/en/inspectorate/staff-and-contacts. The contact info of courts can be found here: http://www.kohus.ee/en/estonian-courts/contacts.