May 2018

EduCluster Finland Ltd. Privacy Policy

General

EduCluster Finland Ltd (hereafter ECF) is a company owned by the University of Jyväskylä, JAMK University of Applied Sciences and Jyväskylä Educational Consortium Gradia. The Company specializes in selling Finnish educational expertise.

ECF considers personal data protection highly important, and it is committed to protect the privacy of its clients, personnel and other stakeholders in the best possible way. The purpose of this Privacy Policy (hereafter Policy) is to outline the rules and practices related to personal data protection followed at ECF. This Policy also serves as a means to demonstrate compliance with the EU General Data Protection Regulation (GDPR).

This policy has been approved by the ECF Executive Team on the 14th of May 2018.

Privacy principles

When collecting personal data ECF shall present data subjects a privacy notice, which outlines the key principles of the data collection. Data subjects shall also be given access to the records of the processing activities containing the rights of the data subject and other detailed information of the data collection. ECF´s client contracts shall contain terms regulating processing of personal information.

The purpose for which data is collected is always defined before initiating data collection.

The necessity of personal data collection will always be evaluated before collecting data. Unnecessary data will not be collected.

A data subject may always request to inspect her/his data and request correction or completion of her/his data. The data subject may also request ECF to restrict data processing, object processing or request her/his data to be erased. Erasure, restriction and objection requests will be complied unless processing of such data is necessary for ECF´s operations and there are legal grounds for processing. A reasoned written decision is always delivered to the data subject if the request cannot be fully complied with.

ECF uses state-of-the art technical measures to protect personal and otherwise confidential information.

ECF does not use automatic profiling or any automated means in decision making concerning natural persons.

ECF data collection in practice

ECF collects and records data of its employees, clients and potential clients, job applicants and external experts who have an interest in ECF´s upcoming projects. ECF´s database of external experts is called Expert pool. Data of job applicants is stored in the Recruitment Filing System.

A default expiry date for the information in the Expert Pool and Recruitment Filing System has been defined. Reminders of updating personal information and renew consent to keep one´s data registered are sent to Expert Pool members when their data expiry date is approaching. Storage time of personal information received from the clients is defined taking into account the actual need. For instance, any travel documents needed for attending a study visit in Finland will be removed after the visit is over. Employee data is updated and removed on an ongoing basis.

ECF website does not collect personal information, unless a visitor decides to contact ECF via the website. ECF does not collect personal information from the visitors or followers of its social media accounts (in addition to what the service providers already collect).

Data Protection Officer (DPO)

A data protection officer (hereafter DPO) is appointed by the Chief Executive Officer of ECF (CEO). The contact details of the DPO can be found on ECF website and on each record of processing activities. The name of the DPO is communicated to the Office of the Data Protection Ombudsman.

Data protection officer shall monitor ECF´s compliance with GDPR and be responsible for maintaining the personal data protection related internal and external instructions. DPO shall respond to general data protection related queries and to the requests of the data subjects. DPO is supported by a legal counsel and an IT expert.

Data Protection officer reports to the CEO regularly when data protection related actions are needed. An annual report concerning the state of data protection at ECF, shall be compiled by the end of February. The annual report shall include at least following:

- evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
- any changes in the nature or amounts of data processed
- data protection impact assessments updates
- list of data protection breaches (if any)
- suggestion for improvements.

Contracts with data processors

ECF only utilizes data processors who are able to meet the requirements of data protection legislation and ensure the protection of the rights of the data subject. There are written contracts in force with all processors.

Data security

ECF monitors that technical measures to safeguard integrity of personal information are up to date.

Sharing of documents consisting essentially of personal information is either done by uploading the document into a cloud-based, username and password protected secure repository or sending them using a secure e-mail system.

A classification of different categories of personal data is compiled. Additional caution will be paid to processing of special categories of data, i.e. sensitive personal information.

Transfer of personal data outside EU

ECF´s clients are mostly located outside EU. ECF currently has a branch in Qatar and in Abu Dhabi. This means that there is a constant need to process and transfer personal information, as well as other information, outside EU. Special attention shall be paid to ensuring that these transfers are done in compliance with data protection legislation. A data protection impact assessment (DPIA) concerning these transfers has been made. It will be updated if changes arise.

Internal controls

Duties of different employees are recognized and documented.

Collection and processing of new type of personal data or acquisition of new it-systems including personal data processing shall be preceded by discussions with the DPO or legal counsel.

Compliance with this Policy shall be evaluated when changes to personal data processing operations are planned. In case of non-compliance, the envisaged change shall be rejected, or this Policy amended.

Sharing knowledge

Staff will be informed of any legislative changes affecting the processing of personal data. The staff will also be informed of any relevant changes of work methods, such as IT systems and personal data processing procedures.

All new employees will be required to familiarize themselves with ECF´s privacy policy, different types of personal information processed by ECF and their roles and responsibilities.

In addition to data protection training on a more general level, practical everyday data protection tips are given. Tailored training for a particular role will be arranged if deemed necessary.

Continuous discussion and improvement initiatives are encouraged. Each staff member has an obligation to report perceived data protection deficiencies to the DPO.

Data protection breach

The security arrangements taken by ECF target at avoidance of data protection breaches. Should a breach occur, measures to repair the perceived deficiency and mitigate the damages will be initiated swiftly.

The reasons of the breach will be investigated and analyzed. Necessary reparatory measures will be taken to avoid such incidents in the future.

Breach will be evaluated by the DPO who shall consult those members of staff who have the most knowledge of the issue.

Transparency

This privacy policy and its subsequent changes will be available on ECF website. In addition to that, ECF will also publish its records of processing activities.

Further Documentation

Public

- Records of processing activities

Internal

- Duties of employees in relation to personal data processing
- List of access rights to network drives and it-systems (maintained by ECF or external network drive service provider)
- Guidelines for using secure e-mail
- A classification of different categories of personal data
- DPIA concerning transfers of data to third countries
- General data processing guidelines and list of everyday practical data protection measures and best practices
- Procedure followed if a data breach is noticed