

Privacy Notice – Recruitment

1. Controller	Name: EduCluster Finland Ltd (ECF)
	Address: Lutakonaukio 7, 40100 Jyväskylä, Finland
2. Controller's authorized representative	Jyrki Saarivaara, CEO Tel: +358 40 1363900 E-mail: jyrki.saarivaara@educluster.fi
3. Contact person	Name: Suvi Geier, Director, Human Resources
	Address: Lutakonaukio 7, 40100 Jyväskylä, Finland
	Other contact information: Tel. no: +358 40 765 5705 E-mail: suvi.geier@educluster.fi
4. Data Protection officer	Name: Suvi Geier Contact information as above
5. Purpose for processing personal data	Personal data will be used in recruiting new personnel. Failure to provide personal data prevents ECF from processing the application.
6. Legal basis for processing the data	GDPR Article 6 subparagraph 1b "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."
7. Description of the categories of data subjects and of the categories of personal data	The applicants (data subjects) have sent an application for employment to ECF. The following information of the applicants may be collected: <ul style="list-style-type: none"> • first name, surname, title, personal identification information • home address • e-mail address, phone number, other contact information • Information/certificates of education and other qualifications • Information/certificates of work experience • CV • immigration related documents • any other recruitment related additional information the applicants have provided unsolicitedly or on request by ECF. • photo, video or audio records made during the recruitment process

8. Regular sources of information	Information is collected from the applicants.
9. Categories of recipients to whom the personal data have been or will be disclosed	<p>Information will be used by ECF's employees who are involved in the recruitment process.</p> <p>The applicant's consent will be asked in advance if ECF would like to give the applicant's personal data to third parties for aptitude evaluation purposes.</p>
10. Recipients in third countries or international organizations	<p>Personal information may need to be transferred outside Europe</p> <ul style="list-style-type: none"> - to a country where the work position applied for, and/or Client, is located. Personal data will not be sent to the Client without consent of the applicant. - to ECF's a branch in Qatar or in the United Arab Emirates or to its representative office in China. Information transfer may need to be in case experts are sought for ECF duties in those countries or if ECF employees based in those countries have essential knowledge needed for evaluating the expert. <p>Data protection legislation in the UAE, Qatar, China and in the home countries of ECF clients differ from GDPR standards. ECF strives to afford the same level of data protection in Europe and outside Europe by using internal guidelines. ECF's clients are informed of the GDPR data processing requirements.</p> <p>The transfer of data is not possible based on the primary mechanisms defined in GDPR articles 45 (commission adequacy decision), 46 (appropriate safeguards) or 47 (binding corporate rules).</p> <p>The legal basis of transfer to ECF Clients is based on GDPR Art. 49 subparagraph 1a "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".</p> <p>The transfer to ECF personnel outside EU is based primarily on explicit consent or exceptionally on GDPR Art. 49 subparagraph 1b "the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request</p>
11. Time limits for erasure of data	<p>Data will be erased two years after the recruitment decisions have been given to the applicants.</p> <p>Unsolicited applications or CVs will not be stored. In case we don't have a suitable open position, ECF will guide the applicant to add the application data to our Expert Pool system.</p>

12. General description of the technical and organizational security measures	<p>A Manual information Information is stored in electronic format. If an extract of the data is produced on paper, the prints will be stored in lockable cabinets.</p> <p>B Electronically processed information The server's database and content files are protected according to following practice:</p> <ul style="list-style-type: none"> • the data is transferred using data encryption (SSL) • the data is backed up on daily basis • access to the data server is restricted to authorized personnel only • access to the data center [physical location of server(s)] is restricted to authorised personnel only <p>Access to the information is controlled by username and password.</p>
13. Rights of the data subject	<p>The data subject has the following rights:</p> <ol style="list-style-type: none"> 1. Right to be informed of data processing (Art 13) 2. Right of access (Art 15) <ul style="list-style-type: none"> - the data subject is entitled to access the personal information processed by the controller and certain information related to the processing 3. Right to rectification (Art 16) <ul style="list-style-type: none"> - the data subject has a right to request correction of inaccurate data and complement incomplete data concerning him or her. 4. Right to erasure (Art. 17) <ul style="list-style-type: none"> - the data subject has a right to request his/her data to be erased 5. Right to restriction of processing (Art 18) <ul style="list-style-type: none"> - the data subject is entitled to obtain from the controller restriction of processing where the conditions in Art 17 are met 6. Right to data portability, if the conditions in Art 20 are fulfilled 7. The right to lodge a complaint with a supervisory authority (Art 77) <ul style="list-style-type: none"> - every data subject shall have the right to lodge a complaint with a supervisory authority (The Office of the Data Protection Ombudsman). <p>The rights may be exercised by contacting the data protection officer.</p>
14. Automated individual decision-making	<p>The information will not be used for automated decision-making producing legal effects concerning the data subjects.</p>