RECRUITMENT PRIVACY POLICY

1. CONTROLLER
   Efore Plc (0195681-3), Linnoitustie 4 B, 02600 Espoo, Finland, tel. +358 9 478 466

2. CONTACT PERSON FOR THIS REGISTER
   Samuli Räisänen, Efore Plc, Linnoitustie 4 B, 02600 Espoo, Finland, tel. +358 50 407 7034, samuli.raisanen@efore.com

3. PURPOSE AND CRITERIA FOR PROCESSING PERSONAL DATA

Data subjects	Purpose of data processing	Criteria
Job applicants	Identifying candidates for open positions and positions that may come available	Consent of an applicant

We process information ourselves and use subcontractors that process personal data on behalf of us. We have outsourced our website IT management to a service provider who administers and secures the server where the data is stored.

Our service providers are Karhu Helsinki (website IT management), Ch5Finland (hosting), Microsoft (email/O365 services) and Google (www-analytics).

4. CONTENT OF THE REGISTER

The register may contain the following information in the job application and curriculum vitae:

Data	**Applicant**	**Purpose of use**
Name	Yes	Identification, communication
Telephone number	Yes	Communication
Email address	Yes	Communication
Work and educational history	Yes	Selection and recruitment
Salary request	Yes	Selection and recruitment
IP address	Yes	Communication

5. REGULAR SOURCES OF INFORMATION

Personal data is collected from the data subject i.e. applicant himself/herself.

6. RELEASE OF INFORMATION

As a general rule, personal data is not released for marketing purposes outside Efore Plc.

7. TRANSFER OF DATA OUTSIDE EU/EEA

Where possible, the data is stored in selected and secure data centers located in Europe. Some of our service providers (Section 3) may use backup servers located outside the EU and EEA in the United States. We have made sure that our service providers are committed to the so-called Privacy Shield frameworks (https://www.privacyshield.gov/list) designed by the EU and the United States to ensure that the data transmitted from Europe to the United States is processed in compliance with data security practices.

8. PRINCIPLES FOR THE PROTECTION OF DATA FILES AND DURATION OF DATA PROCESSING

Safe and secure data processing is important for us. We have employed the following means to secure the protection of data files:

- Access to the system requires a user ID and a password
- The system is protected by firewalls and other technological means
- Data files can only be accessed and used by employees of the Controller who are designated and appointed for the task
- Use of the register is protected with user-specific IDs, passwords and access rights
- The register is located on a server in an ICT room protected from unauthorized access
- The facilities are locked and guarded
- The data files are backed up regularly

As a general rule, personal data is stored as long as it is necessary for the purpose of recruitment. Job applications and CVs sent via this site are deleted automatically within one (1) year after being submitted taking into account the applicable legislation.

9. RIGHT OF ACCESS AND RIGHT TO REQUIRE RECTIFICATION

The data subject has the right to access her/his personal data stored in the register. The data subject has the right to require rectification or erasure of his/her personal data. The data subject also has the right to withdraw his/her consent.

10. OTHER RIGHTS AS A DATA SUBJECT

The data subject has at any time the right to require rectification, erasure or limitation of processing of inaccurate, unnecessary, incomplete or outdated personal data.

The data subject has at any time the right to prohibit using his/her personal data for direct marketing purposes. We never sell or otherwise transfer personal data to third parties in order for them to initiate direct marketing campaigns.

All requests and requirements concerning sections 9 and 10 should be submitted personally or in writing to the contact person for this register mentioned in section 2. The data subject also has the right to lodge a complaint with the supervisory authority if he/she feels that we are violating existing data protection legislation when processing his/her personal data.