

RECRUITMENT PRIVACY POLICY

Pursuant to Article 13 of EU Regulation 2016/679 (GDPR)

1. GENERAL INFORMATION

Epassi Group respects your privacy and is committed to protecting the privacy of all persons interacting with us.

This Recruitment Privacy Policy applies to all candidates applying for a position within the Epassi Group ("**candidate**" or "**you**") and describes how Epassi processes candidates' personal data: what types of personal data are collected, for what purposes they are used, and with whom they may be shared.

In this context, personal data means any information relating to you ("**data subject**") that identifies or can be used to identify you directly or indirectly. Personal data, data subject, controller and other key terms have the same meaning as in the General Data Protection Regulation (2016/679, "**GDPR**"). The Epassi Group and all its companies comply with the GDPR and with other applicable national and EU data protection legislation.

2. CONTROLLER

For the purposes of this notice, the controller of your personal data is the Epassi Group company conducting the recruitment, jointly with Epassi Group Oy. If you choose to allow your application to be considered for other vacancies within the Group, each recruiting company processing your personal data will act as a joint controller together with Epassi Group Oy. For any questions relating to the recruitment process, please contact the recruiting manager indicated in the job posting.

3. CONTACT INFORMATION

Email: dataprivacy@epassi.com

Data Protection Officer (DPO): Taika Pöntinen

4. PERSONAL DATA PROCESSED, PURPOSES AND LEGAL BASIS

Epassi collects only personal data that is relevant and necessary for the purposes of the recruitment process. The following categories of personal data may be processed, to the extent provided by the candidate:

- **Basic and contact information:** name, date of birth, phone number, email address, nationality, gender, address, photo.
- **Identification data:** tax code or passport/ID document.
- **Competences:** educational qualifications, employment history, completed training, language and other skills.
- **Role information:** type of employment, job roles applied for, expected remuneration.
- **Application documents:** cover letter, curriculum vitae. The candidate determines the content of these documents.
- **Other information:** recruitment process status, email communications. We may also collect information from referees indicated by the candidate.

The legal bases for processing are as follows:

- **Collection and management of the application: legitimate interest** of the controller (Art. 6(1)(f) GDPR) in recruiting qualified personnel for open positions.

- **Retention of the application for future vacancies** (where applicable): **consent** of the candidate (Art. 6(1)(a) GDPR), which may be withdrawn at any time without affecting the lawfulness of prior processing.
- **Conclusion of an employment contract**: performance of a **contract** between the controller and the data subject (Art. 6(1)(b) GDPR).
- **Verification of identification or work permit requirements**: **legal obligation** and legitimate interest (Art. 6(1)(c)-(f) GDPR).

5. SOURCES OF PERSONAL DATA

Personal data is generally collected directly from the candidate. Providing personal data is not mandatory; however, without it, it will not be possible to process the application.

With the candidate's permission, we may also collect information from publicly available sources (e.g. LinkedIn profile, other professional platforms) and from referees or recruitment consultants indicated by the candidate.

6. PARTIES INVOLVED IN PROCESSING AND INTERNATIONAL TRANSFERS

The controller uses **Jobylon AB** (Sweden) as its applicant tracking system (ATS). As part of the recruitment process, candidates may be asked to register in Jobylon, or their data may be uploaded to the service with their permission. For further information, please see **Jobylon's Privacy Policy**.

As part of the recruitment process, Epassi may use artificial intelligence tools to assist in the evaluation of applications. Such tools may process candidate data contained in application documents (including CVs and cover letters) and in the records of recruitment interviews conducted by Epassi staff. No decision to advance or exclude a candidate is based solely on the output of an AI tool: human oversight is exercised at every stage of the process. Providers of such tools act as data processors pursuant to Art. 28 GDPR, under Data Processing Agreements (DPAs) that incorporate, where required, the European Commission Standard Contractual Clauses (SCCs) for extra-EEA transfers. Providers are selected among those that ensure candidate data is not used to train their artificial intelligence models.

The controller also uses outsourced cloud-based document management and email services for administrative tasks, and may share candidates' personal data with other Epassi Group companies as part of the recruitment process.

The controller may disclose personal data as permitted or required by applicable law to entities having a legal and/or contractual right to receive it.

When using cloud-based services, personal data may to some extent be processed outside the EU/EEA. The primary storage location is within the EU/EEA. Where data is transferred outside the EU/EEA, the controller ensures that adequate safeguards are in place, including Standard Contractual Clauses adopted by the European Commission.

7. RETENTION OF PERSONAL DATA

Personal data will be processed for the duration of the recruitment process and retained for a further **two (2) years** after the process ends. If the candidate is hired, application data will be retained as part of the employee profile in accordance with the Employee Data Protection Policy.

We regularly assess the necessity of data retention in accordance with applicable laws and will correct or erase inaccurate or outdated data without undue delay. Personal data may be retained for longer periods where required for legal proceedings or administrative purposes.

8. PROTECTION OF PERSONAL DATA

Epassi's Security Management System is based on applicable laws, regulations and international standards (including ISO 27001) and includes appropriate technical, administrative and organisational measures to protect personal data against unauthorised access, disclosure, destruction or other unlawful processing.

Access to recruitment data is limited to those involved in the process. All service providers are required to maintain appropriate data protection measures.

9. YOUR RIGHTS AS A DATA SUBJECT

As a data subject, you have the following rights:

Your right	When applicable
Access: receive a copy of your personal data	Always
Rectification: correct inaccurate or incomplete data	Always
Erasure: request deletion of your data	Where consent has been withdrawn or one of the conditions under Art. 17 GDPR is met
Withdraw consent	Where processing is based on consent
Object to processing	Where processing is based on our legitimate interests
Restriction of processing	Where accuracy of data is contested or another condition under Art. 18 GDPR is met
Human review of AI assessment – right to ensure that no decision on your application is based solely on automated processing	The controller guarantees that any AI-generated assessment is always reviewed by a human recruiter before any determination is made. You may at any time request human review of your individual assessment.

If you are dissatisfied with the handling of your request or any other matter relating to the processing of your personal data, you have the right to lodge a complaint with the competent data protection supervisory authority.

The competent supervisory authority varies depending on the country where the recruitment process takes place. Each candidate has the right to contact the data protection supervisory authority of the country where they habitually reside, work, or where an alleged infringement has occurred. A list of European supervisory authorities is available on the EDPB website: <https://www.edpb.europa.eu>.

Please submit requests for access, rectification or other rights in writing (by email) to the contact listed in Section 3. The identity of the requester will be verified before the request is processed. The controller will reply within the time limits set by the GDPR (as a general rule, within one month). Processing of requests is free of charge; however, manifestly unfounded or excessive requests may be subject to a reasonable fee or refused (Art. 12(5) GDPR).

10. CHANGES TO THIS POLICY

The controller may update this Privacy Policy at any time, for example by publishing a new version on its website. Data subjects are encouraged to review the policy periodically.