PRIVACY POLICY

Job applicant register

1. Controller

Cerion Solutions Oy
Läntinen Rantakatu 53 A, 20100 Turku, Finland
Tel. +358 2 230 1212
www.cerion.fi
Business ID: 2000757-6

2. Person responsible for the filing system

CEO Altti Raali, tel. +358 40 557 3047, altti.raali@cerion.fi.

3. Name of the filing system

Job applicant register.

4. Purpose of processing personal data

The filing system contains applications and CVs sent by job applicants.

5. Content

The filing system contains the following information:

- job applicant's first and last name
- email address
- date and time when the application was received
- information on processing the application
- application
- CV.

6. Data sources

The data in the filing system is collected from the applications submitted by job applicants.

7. Disclosure of data

The data is not disclosed to parties outside Cerion Solutions Oy.

8. Disclosure of personal data outside the EU/EEA

No data will be disclosed outside the EU/EEA.

9. Protection of data

The filing system is protected by user identification, password and access rights. The filing system's system administrators centrally manage access rights through user groups. The administrators of user groups cannot access the filing system without the required access rights. Only the filing system's owner is authorised to request the granting or removal of access rights. The filing system is maintained in a Microsoft O365 environment. The data processed is located in the EU.

More information: https://products.office.com/fi-fi/business/office-365-trust-center-welcome

10. Right of access to personal data

- Data subjects have the right to access their personal data in the filing system. Written copies of the data will be provided upon request. Access to and copies of the data are free of charge, if at least one year has passed since the previous instance of providing the data subject with access to the data.

- The right of access may only be denied for reasons set out in law. Access may be refused, for example, if providing access to the data could endanger the health or treatment of the data subject or the rights of someone else. If access to the data is refused, the applicant will be issued a written certificate to this effect and the applicant may bring the matter to the attention of the Data Protection Ombudsman:

  Office of the Data Protection Ombudsman,
  P.O. Box 315, 00181 Helsinki, Finland.

  The Ombudsman may order the controller to realise the applicant's right of access.

- A request to have access to one's data shall be made to the person responsible for the filing system by a personally signed or otherwise comparably verified document or in person at the controller's premises.

Requests should be sent or delivered to:

Cerion Solutions Oy
Läntinen Rantakatu 53 A
20100 Turku
Finland

11. Right to rectification

- The controller shall, on its own initiative or at the data subject's request, without undue delay rectify, erase or supplement any unnecessary, incomplete or obsolete personal data contained in the filing system.

- If rectification is refused, the job applicant will be issued a written certificate to this effect and he or she may bring the matter to the attention of the Data Protection Ombudsman: Office of the Data Protection Ombudsman, P.O. Box 315, 00181 Helsinki, Finland. The Ombudsman may order the controller to rectify the inaccurate data.

- Rectification requests shall be made in writing and addressed to the person responsible for the filing system. The request should specify in detail and justify the data that the data subject wishes to have rectified, the correct form in which the data should appear and the preferred method of rectification.

  Rectification requests should be sent to:

  Cerion Solutions Oy
  Läntinen Rantakatu 53 A
  20100 Turku
  Finland

12. Contact details for Cerion's data protection officer

tietosuoja@cerion.fi

13. Processing of personal data

Job applicants' personal data is processed by personnel in supervisory positions, HR and the specialists taking part in the interviews.

14. Electronic systems in use

Intranet system.

15. Manual material in use

Before an interview, relevant data may be printed out if needed. Any printouts will be destroyed after the interview in accordance with the process defined for the destruction of confidential data.

16. Data storage period

24 months.