PRIVACY STATEMENT

EU General Data Protection Regulation (2016/679), Articles 12-14

Updated: 2025-03-04

This privacy statement describes the processing of Aidian's job applicants' personal data.
We may update or change this privacy policy at any time and, if required by law, we will notify the data subjects thereof.

1. Data controller and/or joint controller	Aidian Koivu-Mankkaan tie 6 B FI-02200 Espoo Finland Tel. +358 10 309 300 Business ID: 1855216-1
2. Contact details for data protection matters	**Data Protection Officer:** E-mail address: dataprotection@aidian.eu Telephone: 010 309 3000 (center) Postal address: Aidian Oy / Data protection issues, Koivu-Mankkaan tie 6B, 02200 Espoo
3. Name of the register	Aidian's recruitment register
4. Processing of personal data **Purpose and legal basis**	Personal data is processed for the selection procedure of new employees and trainees and for the implementation of internal mobility. This information allows us to contact applicants and make decisions when filling positions. If the jobseeker is selected for the position, the personal data provided by the jobseeker in the recruitment process will also be used in establishing an employment relationship and in tasks related to recruitment as applicable. **Legal basis for processing personal data:** • **Legitimate interest of the controller (Article 6(1)(f) GDPR)** ○ The main basis for processing during the recruitment process. ○ Retention of information about applicants not selected to an open position after the recruitment process so we can utilize the information later in other possible open positions. ○ The proportionality of the processing to the interests of the data subject has been verified on the basis of a balancing of interests. • **Contract (Article 6(1)(b) GDPR)** ○ When drawing up an employment contract with the selected job applicant. • **Consent (Article 6(1)(a) of the GDPR)** ○ Collecting information about the job applicant from sources other than the job applicant themselves, such as the job applicant's recommenders, personality and suitability assessments, security clearances, drug testing, and publicly available information, such as Linkedin or another service.
5. Data content of the register	**Talent community/open applications:** • Basic information, such as first name and last name (required), place of residence and language. • Contact information, such as email address (required) and phone number.

	• Suitability information and other information about yourself and your background provided by the job applicant, such as a link to your LinkedIn profile, a photo, information about your skills and experience, education and work history information (so-called open application). **Recruitment process:** • Basic information, such as first name and last name (required). • Contact information, such as email (required) and phone number. • Suitability information and other information about yourself and your background provided by the job applicant, such as a link to your LinkedIn profile, a photo, information about your skills and experience, education and work history information, language skills. • Information related to the job applied for, such as the nature of the employment relationship, salary expectations, start date, driver's license information or other specific information related to the nature of the job. ○ If necessary, information about the references provided by the job applicant (with the job applicant's separate consent). ○ If necessary, information related to personality and suitability assessments, drug testing or security clearances (with the job applicant's separate consent). ○ Any other information that the job applicant has voluntarily provided in connection with the recruitment process. ○ Information regarding the recruitment process, such as information about follow-up interviews or interruptions in the process, and notes made during the process. The jobseeker can decide what information to provide, but refusing to provide some of the above information or not consenting to the assessment process or security clearance, which is a prerequisite for the position being applied for, may in some circumstances mean that the recruitment process cannot proceed with the candidate because the candidate's suitability for the job cannot be properly assessed.
6. Sources of information	As a rule, the job seeker themselves provides the personal data processed in the recruitment process to the controller. In addition, the data consists of data stored in the recruitment process. With the job seeker's consent, information necessary for recruitment can also be obtained from other sources of information, such as the job seeker's recommenders. In addition, we may use external recruitment consultants who search for potential employees on our behalf.
7. Disclosures and recipients of data and data transfers outside EU/ETA	The processing of personal data has been outsourced to the following service providers who process personal data on behalf of the controller: • For recruitment system provider ○ The recruitment system utilizes international cloud services, which may transfer data outside the EU/EEA, even though the data is located on servers located in the EU/EEA. Any data transfer outside the EU/EEA will be made using the Commission's Standard Clauses or the EU-US Privacy Shield Framework (DPF) and other appropriate safeguards. • For recruitment consultants • For suitability assessment suppliers. In addition, Aidian may, if necessary, disclose data to competent authorities in order to fulfil legal obligations.
8. Retention period of personal data	Personal data is stored for as long as it is necessary for the purposes of processing personal data or to comply with the controller's statutory obligations. The storage periods take into account, for example, the legal periods for claims and the employer's obligations. **Expert community:** • Data stored in the expert community is stored for 12 months from the time the data was provided or modified.

	Recruitment process: • Data from the recruitment process is stored for 24 months from the time the recruitment process ends.
9. Principles of register protection	Personal data is protected by appropriate technical and organisational measures against unauthorised processing and access. **Manual material:** Possible manual material is stored in a locked space that can only be accessed by authorised persons who have committed to confidentiality. **Electronically stored data:** The protection of the register utilises technical data protection (several security mechanisms, such as access control, firewalls, password arrangements) and electronically stored data can only be accessed by authorised persons who have committed to confidentiality. In addition, organisational safeguards are used, such as appropriate personnel training and instructions on data protection. Aidian has a data breach policy and guidelines that enable us to respond quickly to potential data breach situations. In accordance with the policy, we assess potential risks and, if necessary, notify the Data Protection Ombudsman and data subjects.
10. Automated decision-making	Personal data in the recruitment register is not subject to automated decision-making. However, we may utilize the artificial intelligence of the recruitment system, for example to prepare summaries of notes. Artificial intelligence is used only to support the recruitment process, decisions and choices are always made by the person responsible for recruitment.

11. Rights of the data subject	The data subject has the following rights, described in this section, which the data subject can exercise by contacting the controller using the contact details in section 2. If necessary, we may ask you to clarify your request. Please note that the applicability and scope of your rights are specified on a case-by-case basis in accordance with the EU General Data Protection Regulation and that you may not have the rights mentioned below in all cases. In addition, Aidian Oy may need to request some additional information from the requester so that we can verify the requester's identity or authorization.
	
	• **Withdrawal of consent**
	  ○ You can withdraw your consent at any time by notifying us of your withdrawal using the contact details in section 2. Withdrawal of consent does not affect the lawfulness of data processing carried out before the withdrawal.
	• **Right to information about the processing of personal data and to inspect your personal data**
	  ○ You have the right to information about the processing of your personal data. We strive to provide a comprehensive picture of the processing of personal data in our operations through descriptions of our data protection practices, such as data protection statements. In addition, you always have the right to ask further questions about the processing of your personal data. You have the right to request access to the personal data concerning you from the controller and to receive a copy of that data.
	• **Right to rectification**
	  ○ If our personal data concerning you is incorrect or incomplete, you have the right to demand that the data be corrected. If we correct your personal data based on your request, we will, in accordance with the General Data Protection Regulation, inform all parties to whom the incorrect data has previously been disclosed of the correction, if possible.
	• **Right to erasure**

	○ You can request that your personal data be erased in accordance with the General Data Protection Regulation, e.g. if your data has been used unlawfully or the data is no longer needed. However, there is no right to erasure, e.g. if the processing of the data is based on law or the data is needed to establish, exercise or defend a legal claim. The controller may refuse to carry out the erasure on grounds provided for by law. • **Right to restriction of processing** ○ If you believe that we are processing your personal data, for example, unlawfully, incorrectly or you have objected to the processing of your data, you can ask us to restrict the processing of your personal data in accordance with the General Data Protection Regulation. In this case, we can only process the data in limited situations, such as with your consent; for the establishment, exercise or defence of legal claims; for reasons of public interest; for the protection of another person. • **Right to data portability** ○ You have the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format and, if you wish, to have that data transmitted to another controller, where technically feasible. The request can only be made for personal data that is processed automatically and whose processing is based either on your consent or on a contract. • **Right to object to processing** ○ For reasons relating to your specific personal situation, you also have the right to object to processing operations concerning your personal data. In connection with the request, you must identify the specific situation on which you object to the processing. In such a case, we may no longer process your personal data, unless there are compelling legitimate grounds for the processing that override your interests, rights and freedoms, or if the processing is necessary for the establishment, exercise or defence of legal claims. We may refuse to comply with a request to object on the grounds provided for by law. • **Right to lodge a complaint with a supervisory authority** ○ o You have the right to lodge a complaint with a competent supervisory authority, in particular in the EU Member State where you have your habitual residence or place of work or where the alleged infringement has occurred, if you consider that the processing of personal data concerning you infringes data protection law. In Finland, the supervisory authority is the Office of the Finnish Data Protection Ombudsman (current contact details www.tietosuoja.fi). You can also obtain more information about the processing of personal data and your rights from the Office of the Finnish Data Protection Ombudsman.