

PRIVACY STATEMENT

Record of Processing Activities

EU General Data Protection Regulation
(2016/679), Articles 13, 14 and 30

Updated: 1.9.2020

We may update or amend this Privacy Statement at any time and will notify registrants as required by law. Your right to data portability and/or restriction of processing, if applicable, will become applicable as of May 25th, 2018.

This privacy statement describes the processing of Aidian Oy job applicants' personal data. The table below shows the identity and contact details of the controller or processors.

1. Controller / Company	Aidian Oy Koivu-Mankkaan tie 6B 02200 Espoo Finland Tel. + 358 10 309 3000 Company Identification Number: 1855216-1
2. Contact details	Data Protection Officer e-mail: dataprotection@aidian.eu Data protection / Aidian Koivu-Mankkaan tie 6B 02200 Espoo Finland
3. Name of the data file	Aidian's recruitment data file
4. The purpose for processing the personal data / recipients (or categories of recipients) of personal data / the legal basis for processing the personal data	<p>The purpose for processing personal data is to enable the operation of the selection procedure for recruiting company's new employees and trainees, to enable internal mobility and to select members for the organs of the company. Personal data is processed by the persons participating in the recruitment process.</p> <p>The controller may use external services in its operations and in this connection, personal data may be disclosed to the external service provider. Personal data is disclosed in order to obtain outsourced services such as recruitment, video interview and talent assessment services.</p> <p>We may share your information with third parties, such as those who assist us by performing technical operations such as data storage and hosting. If ownership, control of the recruiting company, all, or any part of our products, services or assets changes, we may disclose your personal data to any new owner, successor or assignee.</p> <p>The processing of personal data is mainly based on the consent of the data subject (EU General Data Protection Regulation, Article 6.1.a). In addition, personal data may be processed to a limited extent on the basis of the data subject's legitimate interests (EU General Data Protection Regulation, Article 6.1f) for the purpose of recruitment where a weighting has shown that the data subject's rights and freedoms do not override the data subject's legitimate interests.</p>
5. Content of the data file	<p>The data file may contain information relating to the following groups, when the processing of such data is necessary:</p> <ul style="list-style-type: none">- Applicant's basic information (name, date of birth, contact information)- Job application, CV and other possible information and attachments delivered by the applicant (Including training information, work experience, references, language skills, driving license information)

	<ul style="list-style-type: none"> - Information related to interviews - Video interviews - Information relating to talent and ability assessments - Information relating to security clearance (with the applicant's separate consent) - Information specified in the application process <p>Job applicant can determine what information he or she gives to the recruiting company, however, if he or she refuses to give above mentioned information or will not give a consent to the talent assessment process or security clearance, this can mean in some circumstances that the recruiting company cannot proceed in the recruitment process with the candidate as it cannot assess candidate's performance and suitability for the job in an appropriate way.</p>
6. Source of information	<p>The personal data to be processed is delivered mainly by the job applicant in the recruitment process. For recruiting necessary information may be obtained from other sources with the consent of the applicant. Information relating to security clearance are obtained from the Finnish Security Intelligence Service. Information may also be gathered from the regular operations of the controller.</p>
7. Destinations of disclosed data and whether the data is transferred to countries outside the the European Union or the European Economic Area	<p>By default, personal data will not be transferred nor disclosed outside the European Union (EU) or the European Economic Area (EEA).</p> <p>Possible transfers would concern only such situations, where some of the service provider's servers where data is stored would be located outside of the EU or EEA or the data would be processed outside EU or EEA to fulfil technical support. If this would happen, data is transferred and processed in a legal manner with adequate safeguard.</p>
8. Retention period of the personal data	<p>The controller retains personal data for a maximum period of 1 year unless it is necessary to keep personal data for a longer period in order to fulfill the responsibilities and obligations of the employer company. Personal data related to applicants who have not been appointed to company's organs will be deleted after the member selection process. The data controller destroys the data when the purpose for which they are stored is no longer specified.</p>
9. The principles how the data file is secured	<p>A. Manual data file The manual data shall be stored in an area with restricted access, available only for the authorized persons.</p> <p>B. Electronic information The protection of the data file utilizes technical data protection (several security mechanisms) and electronically stored information is accessible only by the authorized persons.</p>
10. Right of access and right to data portability	<p>The data subject shall have the right of access, after having supplied sufficient search criteria, to the data on himself/herself in the recruitment data file, or to a notice that the file contains no such data. The controller shall at the same time provide the data subject with information of the sources of data in the file, on the uses for the data in the file and the destinations of disclosed data.</p> <p>The data subject who wishes to have access to the data on himself/herself, as referred to above, shall make a request to this effect to the person in charge at controller by a personally signed or otherwise comparably verified document and by verifying his or her identity by attaching a copy of an official identification document.</p> <p>The data subject has the right to data portability, i.e. the right to receive his or her personal data, which the data subject has provided to the controller and that is being processed by automated means, in a structured and machine-readable format and the right to transmit those data to another controller, where the basis for processing is consent or the fulfilment of a contract between the controller and the data subject. Requests for the above uses of the data subject's rights shall be made by contacting the representative of the controller named under section 2 hereof.</p>

<p>11. Right to withdraw consent/ Right to object to processing</p>	<p>In case the legal basis for processing the personal data is the consent of the data subject, the data subject has the right to withdraw the consent.</p> <p>If the processing of personal data is based on the legitimate interest of the controller, the data subject has the right to object to the processing on the basis of his or her specific personal situation. The data subject also always has the right to object to the processing of personal data for direct marketing purposes.</p> <p>The request for withdrawal of consent or opposition to the processing shall be made to the data controller in a handwritten document or equivalent certified document, which shall be presented to the representative appointed by the controller in point 2. Processing of data prior to the withdrawal of consent shall not become unlawful, even if the consent is withdrawn.</p>
<p>12. Rectification, restriction of processing and erasure</p>	<p>A controller shall, on its own initiative or at the request of the data subject, without undue delay rectify, erase or supplement personal data contained in its data file if it is erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing. The controller shall also prevent the dissemination of such information if the information may jeopardize the protection of the data subject's privacy or her rights.</p> <p>The data subject shall have the right to obtain from the controller restriction of processing, in case the data subject has contested the accuracy of the processed personal data, if the data subject has claimed that the processing is unlawful and the data subject has opposed the erasure of the personal data and has requested the restriction of their use instead; if the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or if the data subject has objected to processing pursuant to the EU General Data Protection Regulation pending the verification whether the legitimate grounds of the controller override those of the data subject. Where processing has been restricted based on the above grounds, the data subject who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.</p> <p>If the controller refuses the request of the data subject of the rectification of an error, a written certificate to this effect shall be issued. The certificate shall also mention the reasons for the refusal. In this event, the data subject may bring the matter to the attention of the Data Protection Ombudsman.</p> <p>The controller shall undertake reasonable measures to notify the erasure to the controllers to whom the data has been disclosed and who are processing the data. However, there is no duty of notification if this is impossible or unreasonably difficult. Requests for the above uses of the data subject's rights shall be made by contacting the representative of the controller named under section 2 hereof.</p> <p>The data subject shall have the right to file a complaint with the supervisory authority (the Office of the Data Protection Ombudsman) if the data subject considers the processing of his or her personal data infringes current legislation.</p>