Register Description and Privacy Policy

This is a statement under the EU's General Data Protection Regulation which explains how Desigence Oy processes the personal data of its job seekers in its operations and what the rights of data subjects are.

Data controller

Desigence Oy
Lemuntie 3-5 B
00510 Helsinki
contact@desigence.com

Contact person in matters concerning the register

Arto Ruokonen
Lemuntie 3-5 B
00510 Helsinki
arto.ruokonen@desigence.com
040 501 7095

Name of register

Desigence Oy's job seeker register

Purpose and legal basis of processing of personal data

Personal data of job seekers are processed and maintained for the following purposes on the basis of the job seeker's consent:

- job seeking process (including processing of applications, interviews)
- to carry out possible personal assessments

Personal data of job seekers are not processed for any purposes except for the above. Data are not used for automated decision-making or profiling.

Data content of register

Data to be stored in job seeker register are:

- basic data and data for identification and communication (name, contact information)
- educational data
- data given on job application form and its annexes (such as job history, references, portfolio)
- data related to the job being applied for
- data related to job experience and skills
- recordings from video applications
- possible suitability tests and opinions

Regular sources of data

Data to be stored in a register are obtained from the job seeker, such as from job applications, by email, by telephone or from other circumstances in which the job seeker discloses his or her data.

Retention periods of data

Personal data are kept only for the period of time needed for carrying out the purposes of the data processing. After the time limit the data are removed entirely.

The time limit is:

- 1 month after receiving applications or after an unfavorable selection decision

Regular disclosures of data

Personal data are disclosed only to parties who are legally authorized to receive the data for a specified purpose. These parties include various authorities in a manner separately provided for by law.

Additionally Desigence may use reliable subcontractors in the processing of personal data (such as a partner who carries out suitability assessments or recruitment). In this case, we verify that the service provider takes appropriate security measures and makes sure that processing is in compliance with requirements of the General Data Protection Regulation.

Transfer of data outside of the EU or EEA

Personal data are not transferred outside of the EU/EEA.

Principles of protecting the register

Access to personal data, devices and services are limited to those people whose work requires it. Data are processed by people who have committed to maintain confidentiality.

If a service provider is used to process personal data, data protection legislation and otherwise proper processing of personal data is ensured by contractual arrangements.

Employees are provided with operational guidelines and training on processing of personal data. Compliance with the principles of personal data processing is monitored by means of internal auditing.

Desigence maintains a high level of security in internal networks. Server computers to be used for processing data and locked cabinets containing manual material are located in facilities protected by means of access control and security systems.

Data are backed up regularly. The confidentiality, integrity, usability, data access and fault tolerance of processing systems and services are ensured by, among other things, security updates and by regularly auditing the systems.

Rights of data subjects

Data subjects have the following rights; please submit requests to exercise these rights to the address contact@desigence.com.

Right to review

The data subject may review the personal data we retain.

Right to rectify data

Data subjects may request that inaccurate or incomplete information about them be rectified.

Right to object

The data subject may object to the processing of personal data if he or she believes the personal data have been processed unlawfully.

Direct marketing ban

The data subject has the right to prohibit the use of data for direct marketing.

Right to erasure

The data subject has the right to request the removal of data if the processing of data is not necessary. We process the removal request, after which we either remove the data or give a justified reason for why the data cannot be removed.

It should be noted that the data controller may have a legal or other right to not remove the requested data. The data controller has the obligated to retain accounting records according to the period of time (10 years) specified in the Accounting Act (Chapter 2, Section 10). Therefore material related to accounting cannot be removed before the time limit expires.

Withdrawal of consent

If the processing of personal data related to a data subject is based solely on consent, and not on a customer relationship or a membership, for instance, the data subject may withdraw consent.

A data subject may appeal a decision to data protection ombudsman

A data subject has the right to request that we limit the processing of disputed data until it the matter is settled.

Right of appeal

The data subject has the right to submit a complaint to a data protection ombudsman if he or she believes that we are in violation of valid data protection legislation in our processing of personal data.

Contact information of data protection ombudsman: www.tietosuoja.fi/fi/index/yhteystiedot.html