DATA SECURITY GUIDELINES FOR JOB APPLICANTS

These Data security guidelines (hereafter "Guidelines") explain how Oy Darekon Ltd gathers, manages and shares personal data in connection with job applications and the recruiting process.

1. REGISTRY MANAGER

As per applicable data security directives, the registry manager, Oy Darekon Ltd (hereafter Darekon), is responsible for managing your personal data in compliance with these guidelines and applicable data security directives.

Contact for registry manager
Oy Darekon Ltd
Business ID 0604833-9
Address: Vaisalantie 2, 02130 Espoo
Phone: +358 20 799 1420
Person responsible for data security:
Jorma Miettinen
Address: Vaisalantie 2, 02130 Espoo
email: jorma.miettinen@darekon.fi

2. COLLECTION OF PERSONAL DATA

In most cases we ask you directly for your personal data.

We gather and handle personal data related to applicants that are essential in handling job applications and in the recruiting process, for example

- **basic information,**e.g. name, home address, email, phone number, place of birth
- **information in your job application and related documents,** e.g. education, prior work experience, degrees, language proficiency and references; and
- **data gathered and handled during the recruiting process,** e.g. data related to progress of the recruiting process, notes regarding the application and possible interviews, suitability tests when necessary as well as references.

3. PURPOSE AND LEGAL BASIS FOR HANDLING PERSONAL INFORMATION

We handle applicants' personal data in the recruiting process, for example for handling job applications, informing candidates about the progress of the recruiting process, setting up interviews as well as testing professional or personal suitability. The legal basis for handling of personal data is the possible need to perform measures preceding a work agreement based on the application you have sent us.

4. TRANSFER AND SHARING OF PERSONAL DATA

We may share personal data within the Darekon Corporation. A company owned by the Corporation may handle your personal data on our behalf. The basis for such handing of data is based on our legal right to transfer personal data between companies in the

Corporation for internal management purposes, e.g. reporting and conducting business operations in an effective way by utilising a centralised recruiting system.

We may also provide personal data to third parties with your consent; e.g. to your references and to the person who performs your suitability assessment.

5. TRANSFER OF PERSONAL DATA OUTSIDE THE EU OR THE EEC

We do not transfer personal data handled during the recruiting process anywhere outside the EU or EEC.

6. STORAGE OF PERSONAL DATA

We store pending applications for 12 months after receipt of the application.

Otherwise we store personal data for the duration of the recruiting process. Personal data may also be stored as necessary after the end of the recruiting process to the extent allowed or required by applicable regulations. We usually store personal data for 2 years after the end of the recruiting process.

Personal data are always deleted when their storage is no longer necessary by law or to fulfil the rights and responsibilities of either party.

7. YOUR RIGHTS

You have the right to review your personal data. You may also request that your personal information be corrected, updated or deleted at any time. Note, however, that personal data that are essential to fulfil the uses described in these Guidelines or that must be stored in accordance with law cannot be deleted.

You have the right to object to or limit the use of your personal data to the extent applicable by law.

In certain situations you also have the right to transfer information that you provided to us from one system to another, e.g. the right to access your personal data in a parsed, commonly used, electronically readable form and to transfer your personal data for another registry manager as per applicable law.

We handle your personal data with your consent and you have the right to revoke that consent at any time. Thereafter we will not use your personal data unless there is another legal reason for such use.

You can invoke your rights by sending us a request to the email address jorma.miettinen@darekon.fi

If you feel that management of your personal data is inappropriate, you have the right to make a complaint to the person in charge of data security. Contact information is available at [http://www.tietosuoja.fi/fi/index.html].

8. DATA SECURITY

We implement measures (including physical, digital and administrative measures) that are adequate to prevent the loss, destruction, abuse and unauthorised access or surrender of

personal data. For example, personal data can be accessed only by personnel who require them to perform their work.

Note that even adequate measures cannot prevent all possible data security breaches. In case of a breach in security of personal data we will inform you as per applicable regulations.

9. CHANGES TO THE GUIDELINES

We reserve the right to change these Guidelines. The most recent version of the Guidelines can be found on our website or on the Intranet.

10. CONTACT US

You can enquire about these Guidelines or about management of your personal data by contacting jorma.miettinen@darekon.fi