Recruitment register privacy statement

Drafted on 21 December 2018

1. Controllers

The joint controllers are

Innovation Funding Agency Business Finland (business ID 0512696-4) (hereinafter "**Innovation Funding Agency**"); and

Business Finland Oy (business ID 2725690-3) (hereinafter "**Company**")

Porkkalankatu 1
FI-00101 Helsinki

P.O. Box 69, FI-00101 Helsinki (Innovation Funding Agency)
P.O. Box 358, FI-00181 Helsinki (Company)

Tel. +358 29 505 5000

2. Contact person and contacts

The contact persons for the recruitment register are Heidi Elvilä (Innovation Funding Agency) and Eetu Lillrank (Company)

Data subjects may submit enquiries or exercise the rights described in Section 2 of this privacy statement by contacting the contact persons for the joint controllers by email at firstname.lastname@businessfinland.fi or tietosuoja@businessfinland.fi. Data subjects are advised to primarily contact the joint controller with whom they have an employment relationship or other contractual relationship or at which they are applying for the position.

3. Name of filing system

Innovation Funding Agency Business Finland and Business Finland Oy recruitment register

4. Purpose and legal basis of personal data processing

The Innovation Funding Agency and the Company have merged their human resources administration and therefore maintain a joint recruitment register. Open applications and other personal data submitted by the applicant may be used in the recruitment process of either of the organizations. Both organizations' representatives take part in the recruitment process and handling of personal data therein.

The Innovation Funding Agency and the Company act as joint controllers and jointly determine the purposes and means of processing personal data in the filing system. The controllers are jointly responsible for compliance with the EU General Data Protection Regulation in processing personal data in the filing system. The joint human resources administration acts as the legitimate interest under the EU General Data Protection Regulation by which the Innovation Funding Agency and the Company may process the personal data of employees and contracting partners of both parties, as well as the personal data of each others' job applicants.

Processing of personal data applies to persons who have applied for open job or public office in the Innovation Funding Agency or in the Company, or submitted an open application to the Company. The Innovation Funding Agency's and the Company's legitimate interests constitute the legal basis for the processing of the personal data as required in the recruitment process in the factual connection between the applicant and the Innovation Funding Agency or the Company. The personal data is utilized in the evaluation of the applicant and in the recruitment decision making.

If required by the law, the Innovation Funding Agency or the Company asks the data subject for consent to collect or process certain type of personal data. Consent may be asked for example for performing security clearance or competence testing. Competence testing may include profiling.

Processing tasks may be outsourced to the controllers' third-party service providers, as provided for in and in compliance with data protection legislation.

If the data subject is recruited to the Innovation Funding Agency or the Company, his/her personal data may be transferred to the joint employee register of the Innovation Funding Agency and the Company.

5. Data content of the filing system

The data stored in the filing system depends partly on what type of information the applicant has submitted in the application or in supportive documents. The following types of data can be stored on data subjects:

Name, date of birth, sex, address, other contact details, nationality, education and work experience, other personal data presented in the application or in the supportive documentation such as CV, personnel record or results of competence testing and analyses, data related to security clearing and/or credit report, education or examination certificates, testimonials, contact persons indicated by the applicant for referrals, and other necessary information related to the application or fulfillment of eligibility criteria of the public office.

Information that is needed in completion of tasks and duties provided by the employment contract may be stored, too. Such tasks and duties may include e.g. payment of salaries and this type of information may include e.g. identification number and bank account number for paying salary.

6. Retention period of personal data

The retention periods of personal data in the filing system are based on legislation, and may vary depending on the type of data and its purpose of use.

Applications submitted in Valtiolle.fi –system: Applications submitted in individual recruitment processes are deleted from the system six months after the process in question has ended. Open applications are deleted from the system six months after they were last saved. The applicant's personal data is deleted after it has remained unused for one year. The applicant is notified of this before the data is deleted. Applicants may also ask deletion of the personal data by themselves.

Applications submitted in LAURA -system and other applications: As a rule, applications submitted for the specified recruitment process will be destroyed two years after completion of the recruitment process. Information may be processed in the service even longer e.g. in cases where the applicant has been hired as an employee or a stand-in for the organisation. Open applications and the data submitted will be retained at least six months from submission of the application. Personal data related to possible disputes will be retained until the dispute has been irrevocably settled.

Where security clearances contain observations to be reported, the clearances shall be destroyed immediately after processing.

Personal data are destroyed either by erasing the data altogether or by rendering the data passive by ceasing its processing and preventing access by means of either encryption or restriction of access rights.

7. Regular sources of data

Personal data are collected primarily from applicants themselves. Information that is necessary in the recruitment may be collected also from other sources based on the applicant's consent. Possible competence- and other testing may be outsourced to the third-party service providers. When necessary, personal credit reports will be checked from Suomen Asiakastieto Oy.

Data related to the recruiters' access rights are collected based on the human resources planner's access right requests.

8. Regular disclosures of data and groups of recipients

Personal data may be disclosed only within the limits required and permitted under valid legislation or with the consent of the data subject.

The applications for the public office or for fixed term position delivered to the authority are public documents as referred to in the Act on the Openness of Government Activities

(621/1999), and access to them is given on request. The said Act does not apply to other applications than those addressed to the Innovation Funding Agency. Public documents are disclosed according to the conditions set out in sections 13 and 16 of the Act. Access to secret information is given and the information is disclosed only 1) with the permission of the person concerned, 2) to the person concerned or 3) under a right based on the Act.

9. Transfers of data outside the EU and the EEA

Applications submitted in Valtiolle.fi –system: As a rule, no personal data is transferred outside the EU or the EEA.

Other applications: The personal data may be transferred outside the European Union or European Economic Area in accordance with the requirements and restrictions of data protection legislation. Where no decision exists on a sufficient level of data protection in the destination country, the transfer of data shall be carried out in accordance with the standard clauses approved by the European Commission. For further information on the safeguards employed in transfers of data, see the European Commission website.

Furthermore, the personal data may be transferred outside the EU and EEA in accordance with the requirements and restrictions of data protection legislation to employees of the Business Finland international network, subsidiaries and subcontractors of the Company and service providers used for its processing.

10. Principles of protection of the filing system

Manual material

Manual material are processed by trained personnel in locked facilities that correspond to the security classification of the data. Personnel and subcontractors processing the data have a non-disclosure obligation. Materials are destroyed in accordance with the data control plan.

Electronically processed data

The protection of electronically stored data is based on identity and access management, technical safeguards in place for the databases and servers, physical protection of facilities, access control, secure data communications and the maintenance of data backups.

Access to electronic data in the filing system is protected by means of individual usernames and passwords. The right to access and process the data is granted to persons working in HR-department and to the recruiting superiors as well as to other persons on the basis of performance of work duties.

The purpose of the above measures is to safeguard the confidentiality of personal data stored in the filing system, the availability and integrity of the data, and the exercise of data subjects' rights.

11. Automated decision-making

Data in the filing system will not be used for decision-making that has legal effects on data subjects or is based on automated processing activities, such as profiling.

12. Rights of data subjects in personal data processing

Data subject's right to access data (right of inspection)

Data subjects have the right to receive a confirmation that their personal data is processed and access their personal data stored in the filing system. Requests for access must be submitted as instructed in this privacy statement and addressed to the specified contact person. The right of access or inspection may be declined on legal grounds. In principle, using the right of inspection is free of charge.

Data subject's right to request data to be corrected, removed or its processing to be limited

Insofar as a data subject may act independently, they must without undue delay after being notified of an error, or after having detected an error, rectify, remove or supplement the inaccurate, unnecessary, insufficient or outdated data in the filing system. If a data subject is unable to correct the information themselves, a request for correction must be submitted to the contact details given in this privacy statement.

A data subject may also request that the controller limit the processing of their personal data if the data subject is awaiting a response from the controller to a request to correct or remove information, for example.

Data subjects' right to data portability

Insofar as the data have been provided by the data subject and processed on the basis of the consent of the data subject or for performance of a contract between the data subject and controller, data subjects have, as a rule, the right to receive the data in a machine-readable format and the right to transfer said data to another controller.

Data subjects' right to object to processing

On the grounds of special personal circumstances, data subjects have the right to object to profiling and other processing activities by the controller insofar as the basis for processing is the pursuit of the controller's legitimate interests.

Data subjects may submit their objection by contacting the joint controllers at the contact details specified earlier in this privacy statement. It is recommended that data subjects primarily contact that joint controller to whose processing they wish to object. In the objection, the data subject must specify the special circumstances under which they object to

processing. The joint controllers may refuse to comply with the objection to processing on legal grounds.

Data subject's right to file a complaint with the supervisory authority

A data subject is entitled to file a complaint with a competent supervisory authority if a register controller has not followed the applicable data protection regulation in its operations. The supervisory authority in Finland is the Data Protection Ombudsman.

13. Updates

This privacy statement was last updated on 29 June 2022.

As the controller follows changes to data protection legislation and strives to continuously develop its operations, it reserves the right to update this privacy statement.