Privacy statement for Tenderer and Supplier Register

Drafted on 7 September 2020

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-00180 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. Contacts

Data subjects may submit enquiries or exercise their rights as described in this privacy statement by contacting **tietosuoja@businessfinland.fi**.

3. Name of the register

Innovation Funding Agency Business Finland's and Business Finland Oy's Tenderer and Supplier Register

4. Purpose and legal basis of personal data processing

The Innovation Funding Agency and the Company have merged their procurement service and therefore maintain a joint tenderer and supplier register. 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 procurement service 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 each other's tenderers and suppliers.

In the bidding phase the personal data of tenderer's contact persons, members of management and persons offered to perform the service is used for communication with the tenderer, comparison or tenders and verification of other requirements imposed for the procurement (including the requirements imposed in the public procurement legislation). Part of the requirements are checked only against the winning tenderer.

Personal data of **the chosen supplier's** contact person as well as service personnel may be used for communication, performance of the contract and monitoring of the procurement.

The legal basis for processing personal data is contract, when processing is based on preparations or performance of a contract between the the data subject and the controller. In some occasions, the legal basis for processing the personal data is the controller's statutory obligations, such as obligation to check criminal records in the procurements that exceed EU threshold value. In all other cases, processing of personal data is based on the controller's legitimate interest.

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

5. Data content of the Register

In the bidding phase the controller may store following types of data:

- Tenderer's contact person's/managers'/service personnel's name, business contact details, previous job experience and education (service personnel only). In the bidding phase the tenderer may submit CVs on service personnel that may include also date of birth or social security numbers.

In the contract negotiation and performance phase the controller may store following types of data:

- Supplier's contact person's/service personnel's name, telephone number, e-mail address
- The controller checks criminal records as required in the public procurement legislation. The following information is filed about the criminal records check: name of the verified person, position and organization, the person who made the verification in Business Finland
- Security clearance of service personnel, as necessary. Only the information on performance of security clearance is filed.
- Confidentiality undertakings: Name, entity, object of co-operation, signature/name, position in the organization
- If the service personnel get restricted access to the controller's data systems, the controller may, for purposes of information system access management, store similar type of personal data of them as of its own personnel: access rights to information systems, usernames and passwords, other identifying information, log records collected from accessing information systems

6. Retention period of personal data

Personal data included into the tendering and contractual documentation is retained as long as the tendering and contract documents are retained, generally 10 years from the end of the procurement.

The copy of the criminal records shall be destroyed immediately after processing, but information whether criminal record has been checked, will be retained. Where security clearances contain observations to be reported, the clearances shall be destroyed immediately after processing, but information whether security check has been made, will be retained.

The need for retaining the data is assessed periodically, generally at least every five years.

7. Regular sources of data

Personal data are collected primarily from the tenderer, or from the data subjects themselves. Copy of the criminal records is always received from the data subject. Information concerning possible security clearances are received from the Finnish Security Intelligence Service (SUPO).

8. Regular disclosures of data and groups of recipients

No regular disclosures.

9. Transfers of data outside the EU and the EEA

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, or by other legal means or basis of transfer.

The Company may transfer personal data 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.

As a rule, the Innovation Funding Agency does not transfer personal data outside the EU or EEA.

10. Principles of protection of the filing system

Manual material

Manual material are processed by trainer 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 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. 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, or data that is contrary to the purpose of 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. 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 the 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 7 September 2020.
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.

***