Työllisyysrahasto
Sysselsättningsfonden | Employment Fund

23.11.2022

Privacy Statement – Insider Administration and Related Information

1 Controller and contact details

Name: The Employment Fund

Mailing address: P.O. Box 113

FI-00181 Helsinki

Visiting address: Itämerenkatu 11-13, FI-00180 Helsinki

In all questions related to the processing of personal data and in situations related to exercising the data subject's rights, the Compliance Officer acts as the contact person:

E-mail: compliance@tyollisyysrahasto.fi

Tel: +358 (0)9 6803 7380 (switchboard)

Mailing address: Employment Fund, Compliance Officer, P.O. Box 113, FI-00181 HELSINKI

If you have any questions about data protection issues, you can contact the Data Protection Officer of the Employment Fund. Contact details of the Data Protection Officer:

E-mail: tietosuoja@tyollisyysrahasto.fi

Tel: +358 (0)9 6803 7380 (switchboard)

Mailing address: Employment Fund, Data Protection Officer, P.O. Box 113, FI-00181 HELSINKI

2 Name of the register

Register of the executives referred to in the Market Abuse Regulation, their related parties and their transactions, other insiders of the data controller, the scope of trading restrictions, and related parties and related party activities in accordance with the Related Party Guidelines.

3 Purpose and basis of processing

The processing of personal data is based on the task or obligation of the data controller stipulated in the law or determined pursuant to it (EU General Data Protection Regulation, Article

6.1.c). The data controller or a person acting on its behalf has the obligation to maintain a list of persons who have access to inside information and who work for the data controller on the basis of a contract or otherwise perform tasks through which they have access to inside information. The purpose of processing the personal data of executives and persons in their related parties is to comply with the regulation regarding transactions of executives and their related parties in accordance with Article 19 of the Market Abuse Regulation (MAR; EU 596/2014), as well as other laws, rules, regulations and instructions binding on the data controller. The data controller maintains a list of related parties in accordance with the Related Party Guidelines based on the Accounting Act and IFRS standard (IAS 24) in order to identify related party activities and at the same time comply with insider regulations. Since the information related to the preparation of the financial review is particularly confidential, the data controller maintains a list of persons participating in the preparation of the financial reviews, and they are subject to the trading restriction set by the data controller during the closed window referred to in section 2.3.2 of the Stock Exchange's insider instructions.

The data controller shall keep a list of persons in managerial positions and their related parties. A person in managerial position shall be considered to be a person who is:

- Member of the administrative, management, or supervisory board
- a senior-level person who is not a member of the aforementioned body, but who has regular access to insider information directly or indirectly concerning the entity in question and who has the authority to make management decisions that affect the future development and business prospects of the entity in question.

With the criteria mentioned above, the following persons have been defined as persons working in management positions, who and whose related parties are subject to a special obligation to report transactions:

- members of the supervisory board
- members of the Board of Directors
- Managing Director and Chief Financial Officer

The project-specific insider list includes all persons who have access to insider information about the project, and who work for the company or perform tasks for the company through which they have access to insider information about the project. The purpose of processing personal data is to comply with the regulations regarding the transactions of these persons, as well as other laws, rules, regulations and instructions binding on the data controller, in accordance with Article 18 of the Market Abuse Regulation (MAR; EU 596/2014).

The processing of personal data for these purposes is necessary to comply with the statutory obligations of the data controller.

4 What kind of information we collect

The following personal data is processed about executives and their related parties:

- first and last name
- personal identity code and date of birth

- home address, email address, and telephone numbers
- name and address of the employer
- first name, last name, postal address, e-mail address, and telephone number of the authorised person or contact person listed
- position of an executive in the organisation
- the basis for being a related party
- related party entity
- start and end date of the executive/related party disclosure
- reports of transactions received

The insider list contains the following information for insiders:

- first and last name (and surname of birth if different from current surname)
- personal identity code and date of birth
- home address, email address, and telephone numbers
- name and address of the employer
- first name, last name, postal address, e-mail address, and telephone number of the authorised person or contact person listed
- reason for insider status and start and end time (date and time)
- reports of transactions received

The list of persons participating in the preparation of financial reviews contains the following information of the persons included in the list:

- first and last name
- e-mail address
- name and address of the employer

5 Regular data sources

In accordance with MAR, the data controller identifies the persons who have access to the controller's financial information and collects any necessary additional information directly from the person in question. Personal information about executives and their related parties is collected pursuant to MAR from the executive and/or their related parties / contact persons of

the related parties, as well as from entities authorised by them and from public information sources, such as the trade register.

In accordance with MAR, the data controller collects the information entered in the insider list from the data subjects themselves when submitting the insider notification using a separate form to be completed by the data subject and, if necessary, also from public sources of information (e.g. the Trade Register, BIS). Data subjects themselves report their business to the data controller.

The data controller will personally identify persons belonging to a related party in accordance with the instructions and collect any necessary additional information directly from the person in question.

6 Data disclosure and transfer

Personal data may, within the limits permitted and required by the legislation in force at the time, be disclosed to the parties who, under the legislation, have the right to access the data, or if the preparation, presentation or defence of a legal claim requires the disclosure of personal data. For example, information can be disclosed to entities named in the MAR regulation and the rules issued pursuant to it, such as the Financial Supervisory Authority, ESMA, and the Police.

Data shall not be transferred outside the European Union or the European Economic Area, subject to a mandatory legal provision.

7 Retention period of personal data

The retention period of personal data is determined in accordance with the requirements of MAR and other applicable company and securities market legislation. As a rule, the retention period is five years after the registration of personal data or the latest update.

8 Protection of personal data

The personal data in the register is protected in the manner required by legislation, taking care of information security. The data controller has taken appropriate technical and organisational measures to protect personal data against accidental or unlawful loss, disclosure, misuse, alteration, destruction, or unauthorised access.

Data security measures are designed to meet the continuous development of technology. The data is protected by firewalls and various encryption technologies, in addition to which the selected hardware facilities are secure and access control is appropriate. Data in the systems is backed up regularly.

Access to the register is restricted by means of access rights so that the data stored in the system can only be accessed by employees who have the right to do so on behalf of their duties and who need information in their tasks.

9 Rights of the data subject

The registered person has the right to check the personal information concerning them and to receive a copy of this information if they so wish, unless providing a copy endangers the rights and freedoms of others. The data subject also has the right to demand that the data controller rectify, delete, or supplement personal data concerning them that is incorrect, unnecessary, incomplete, or outdated in terms of the purpose of the processing.

Requests for inspection and correction must be addressed to the contact person of the register whose contact details can be found at the beginning of this statement, by sending a signed letter or a document that has been validated in a similar manner to ensure that the person making the request is entitled to the request. If necessary, the data controller may request the data subject to specify their request in writing and, if necessary, the data subject's identity may also be verified before taking other measures. The data controller replies to requests for inspection within one month of the request and, as a rule, submits the information free of charge. However, if data requests made by the data subject are unfounded or unreasonable, such as a person repeatedly making data requests, the data controller has the right to charge a reasonable fee for the collection of data. The fee shall consist of administrative costs incurred for the implementation of the requested measure and the provision of related information. The data subject may choose whether to personally retrieve the data from the data controller's office or to receive the data as a registered letter.

The data subject also has the right to request the erasure of their personal data (the so-called right to be forgotten) when the data are no longer needed for the purposes for which they were collected or otherwise processed, or when there are no statutory obligations to process or store the data. The data controller also has the right to refrain from the erasure of register data when the data controller has a legitimate interest in not deleting such data or when the data concern matters that are necessary for a valid customer relationship, for example.

The data subject has the right to lodge a complaint with the supervisory authority if the data subject considers that the processing of personal data concerning them is in breach of the General Data Protection Regulation.

The contact details and instructions of the Office of the Data Protection Ombudsman can be found here: https://tietosuoja.fi/en/contact-information

We will be happy to assist you with any issues related to the processing of personal data and the exercise of your rights. Please contact us in writing. See section 1 at the beginning of the privacy statement for contact information.

10 Changes in the privacy statement

The data controller is constantly developing its business and therefore the data controller reserves the right to amend this privacy statement by informing data subjects accordingly. Changes to the privacy statement may also be based on changes in legislation.

The data controller informs about changes to the privacy statement on its website by publishing an updated privacy statement and the date on which the changes were made. The privacy statement can also be provided to employees using the internal communication channels used by the data controller at any given time. If the data controller makes significant changes to the privacy statement, information on the matter will also be communicated by other means, such

as sending an e-mail message or publishing it on the web pages and/or social media pages before the changes take effect.