PRIVACY POLICY

Fincoil LU-VE Oy ("Controller") has established a reporting channel in accordance with the The Act on the Protection of Persons Reporting Infringements of European Union and National Law (1171/2022, hereinafter referred to as the Whistleblower Protection Act). This Privacy Notice describes how the Controller processes personal data in connection with the notification procedure under the Whistleblower Protection Act.

The Controller complies with data protection legislation when processing personal data. Data protection legislation refers to the applicable data protection legislation, such as the General Data Protection Regulation of the European Union (2016/679) ("GDPR"), the national Data Protection Act (5.12.2018/1050) and the guidelines and regulations of the supervisory authority. Terms relating to data protection that are not defined in this Privacy Policy shall be interpreted in accordance with data protection legislation.

Name of the register

Notification procedure of Fincoil LU-VE Oy

Purposes and legal grounds for processing

Your personal data is processed for the purpose of processing reports under the Whistleblower Protection Act and investigating reported misconduct.

The processing of personal data is based on Article 6(1)(c) of the GDPR and the statutory obligation of the Controller to establish a channel for reporting misconduct.

The notification can be made anonymously, in which case personal data will not be processed unless the person later provides additional information about their identity. The provision on providing information is mandatory for the identification of the relationship between the notifier and the Controller and for the description of the facts relating to the infringement. Refusal, in whole or in part, to provide this information may render it impossible to process the received notification.

Data content of the register

The register may contain the following types of personal data concerning the notifier and the subject of the report, as well as other persons involved in the matter:

1. Name, email address, telephone number of the notifier. The report can also be submitted anonymously.
2. Information about the report, such as the name of the object, information related to illegal activity (incl. place and time), information related to the making and processing of the notification and messages (incl. the code and status of the notification)
3. Any other information provided by the notifier.

In addition, information is stored about the processors of notifications received through the channel. Such information includes, for example, the person's name, job title, email address, user IDs to the system, log data on the use of the system.

Data retention

The Controller retains personal data in accordance with the aforementioned confidentiality requirements

for as long as it deems necessary for the processing of the report and in any case no more than five years from the receipt of the notification, unless the storage of the data is necessary for the exercise of the Controller's legal rights or obligations or for the establishment, exercise or defence of legal claims.

Personal data that is clearly not useful for processing a particular report will not be processed. If personal data is collected accidentally, it will be deleted immediately.

Regular sources of information

The data is obtained

- from the notifier
- through notifications or additional information sent through the whistleblower channel or notifications or additional information delivered to the Controller in some other way.
- Information systems of the Controller or other sources which are relevant for the processing of the notification

Data processing modalities

Each processing operation of personal data must be carried out in accordance with the GDPR and other applicable data protection legislation.

The processing of data is carried out manually (e.g. on paper) and/or automated (e.g. by means of electronic processes and/or tools) logically suited to the above purposes and in any case in such a way as to ensure the security and confidentiality of the data. At all stages, the notification management system guarantees the content of the report (including information on any third parties included in the report) and the confidentiality of the identity of the notifier, the persons concerned, the persons mentioned in the report and the advisor, including through the use of encrypted communications.

Data processing does not include automated decision-making or profiling.

Contact details of the controller and data protection officer

The Controller is Fincoil LU-VE Oy, whose domicile is Ansatie 3, 01740 Vantaa. The Controller can be contacted at e-mail address whistleblowing.fincoil@luvegroup.com .

The Data Protection Officer is Unindustria Servizi &; Formazione Treviso Pordenone S.c.a.r.l., which can be contacted at dpo.luve@luvegroup.com.

This Privacy Policy complements the website browsing policy and is intended to illustrate to users how the Controller specifically handles the data contained in this contact form. Please read our privacy policy at the following link:

https://exchangers.luvegroup.com/cms/view/home/privacy/s4/c1768?language_code=ENG

Recipients or categories of recipients

Your personal data may be processed by third parties. These parties mainly belong to the following categories:

- Consultants (legal and financial advisors and other experts)
- External parties or parties belonging to the same group as the Controller that cooperate directly with the Controller in the technical and IT administration of the whistleblower channel, as well as other external parties to whom the information must be provided by law.

Transfer of data to a third country and/or international organisation

Your personal data will not be transferred to third countries outside the European Union or EEA.

Right to access personal data and other rights

The data subject has rights under data protection legislation. Please note that the precise application of these rights in each individual situation will depend on the purpose and context of the processing of personal data.

The data subject can send requests concerning their rights by e-mail to:

whistleblowing.fincoil@luvegroup.com

As a general rule, the Controller will not charge data subject a fee for processing the request. However, where the data subject's requests are manifestly unfounded or excessive, such as where they are repeated, the Controller may charge the data subject a reasonable fee based on the administrative costs of processing the request.

Right to access personal data and receive a copy of personal data

The data subject has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed and to obtain information on the processing of personal data as defined in data protection legislation. In addition, the data subject has the right to obtain a copy of the personal data being processed.

However, the right of access of the data subject may be restricted in respect of personal data reported under the Whistleblower Protection Act if this is necessary and proportionate in order to ensure the accuracy of the report or to protect the identity of the whistleblower.

Right to rectification

The data subject has the right to demand the rectification of incorrect or inaccurate personal data.

Right to erasure

The data subject has the right to request the erasure of personal data concerning him or her without undue delay, provided that

- the personal data are no longer necessary for the purposes for which they were collected or

for which they are otherwise processed;

- the data subject withdraws the consent on which the processing was based on and there is no other lawful basis for the processing;
- the personal data have been unlawfully processed; or
- the personal data must be erased in order to comply with a legal obligation under Union or national law.

Right to restriction of processing

Restriction of the processing of personal data means that the personal data subject to the restriction may only be processed in addition to being stored:

- with the consent of the data subject
- for the establishment, exercise or defense of legal claims
- for the purpose of protecting the rights of another natural or legal person
- important grounds of public interest of the Union or of a Member State

The data subject has the right to request the restriction of processing by the Controller where

- the data subject contests the accuracy of the personal data, in which case the processing shall be limited for the time necessary for the Controller to verify the accuracy of the data;
- the processing is unlawful, and the data subject objects to the erasure of the personal data and requests instead the restriction of their use;
- the Controller no longer needs the personal data concerned for the purposes of the processing, but the data subject needs them for the establishment, exercise or defense of legal claims

However, the data subject's right to restrict processing does not apply to the processing of personal data in accordance with the Whistleblower Protection Act.

Right to withdraw consent

Where the processing of personal data is based on the data subject’s consent, the data subject has the right to withdraw his or her consent at any time without affecting the lawfulness of the processing carried out on the basis of that consent. However, the personal data of the data subject may be retained if the retention of the personal data is necessary to comply with a legal obligation imposed on the Controller.

Right to data portability

The data subject has the right to request that the Controller provides the personal data regarding the data subject in question in a structured and commonly used electronic form. The data subject may also request that the personal data is transferred to another controller if this is technically feasible.

Right to lodge a complaint with a supervisory authority

The data subject has the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data concerning him or her infringes the applicable data protection regulation.