ARE Oy's Privacy Statement for Whistleblowing Channel

This privacy statement describes how ARE processes personal data submitted to the company's whistleblowing channel ('whistleblowing channel', 'ethical channel'). ARE complies with legislation applied to the processing of personal data, including the regulations and principles of the European Union's General Data Protection Regulation (2016/679) ('GDPR') and the Finnish Data Protection Act (1050/2018). 'Personal data' or 'data' or 'information' means any information relating to a natural person ('data subject') who can be directly or indirectly identified by reference to said information, as stipulated in the General Data Protection Regulation. Any data protection terminology not defined in this privacy statement shall be interpreted in accordance with the General Data Protection Regulation. This privacy statement pertains to all individuals who submit a report through the whistleblowing channel.

1. Data controller and contact information for matters related to data file

Name: ARE Oy (business ID: 0989493-6)
Kaivokselantie 9
01610 Vantaa, Finland
E-mail: eettinenkanava@are.fi
Phone: +358 20 530 5500 (switchboard from 8 a.m. to 4 p.m.)

ARE Oy's data protection officer can be reached at gdpr@are.fi

2. The purpose and legal basis of processing personal data

Personal data is processed for the purpose of providing the whistleblowing channel and processing submitted reports. The data is used to track and investigate misconduct and, where necessary, to establish, exercise or defend a legal claim or to assist with other requests made by the authorities.

The whistleblowing channel helps ARE ensure that it complies with rules related to its decision-making and monitoring system and with legislation, in particular regarding accounting, auditing, bribery, money laundering, environmental and financial crime as well as competition rules. The whistleblowing channel is managed in accordance with the Act on the Protection of Persons Reporting Infringements of European Union and National Law (1171/2022) ('*Whistleblower Act*'). In this case, the legal basis for processing is the data controller's obligation to comply with legal requirements (Article 6(1)(c) in the General Data Protection Regulation, §6.1, section 2 in the Finnish Data Protection Act).

Through the whistleblowing channel, individuals may also report any breaches of the company's code of conduct and procedural guidelines that may relate to e.g. financial issues, conflicts of interest, bribery, misconduct and other illegal activity. In this case, the basis for processing is the data controller's or a third party's legitimate interest to ensure the legitimacy and ethicality of the operation (Article 6(1)(f) in the General Data Protection Regulation). Where such reports include special categories of personal data, the processing of such data may be necessary for the establishment, exercise or defence of legal claim in accordance with Article 9(2)(f) in the General Data Protection Regulation).

3. Types of data processed and data sources

The data file may include the following personal data regarding the whistleblower and the subject and anyone else associated with the matter, such as witnesses:

- Whistleblower's name, e-mail address and phone number (the report may also be submitted anonymously):
- Reported information, such as the name and contact information of the subject, description, time and location of breach or misconduct and other matters regarded meaningful by the whistleblower (depending on the nature of the report, the processed data may include information regarded as special categories of personal data).
- The names and contact information of any witnesses or other people associated with the matter.
- Any information related to submitting and processing the report as well as communication (incl. status of report).
- Any other information reported by the whistleblower and other information collected during the processing and investigation of the report.

In addition, information on individuals processing the reports submitted through the channel is stored, including name, job title, e-mail address, system login and log entries on system use.

The whistleblower is the primary data source for any information stored in the data file. In addition, the data includes information stored during the processing of misconduct reports, such as information from employees associated with the matter, data from IT systems and information received in a possible hearing of the subject. Other data sources are used within legal limitations. Processing and investigating the reports necessitates provision of personal data. In principle, investigations cannot be conducted without personal data.

4. Disclosure and transfer of data

Any reports received through the whistleblowing channel are processed by an investigative team appointed by ARE. In addition, a very limited number of other individuals may participate in the processing of the report, such as legal advisers, experts authorised by the company and anyone taking part in the internal review.

The whistleblower's identity is not disclosed without their express consent to any individuals other than those in control of report reception and follow-up actions. However, the identity of the whistleblower may be disclosed in accordance with legal requirements if competent authorities require the information for the purpose of verifying the validity of the report, if authorities in charge of preliminary investigations or prosecuting officers require the information to perform their duties or if it is necessary for the establishment, exercise or defence of legal claim. In accordance with legal requirements, we shall notify the whistleblower in advance of the disclosure of their identity, unless such disclosure jeopardises the verification of the validity of the report or any related preliminary investigations or legal proceedings. Otherwise, personal data may be disclosed to authorities and other parties entitled to the information, as required by law. In addition, personal data may be disclosed to third parties if the data controller is involved in an investigation by the authorities, legal proceedings or any other procedure taking place in a dispute resolution body.

We employ a service provider for the administration of the whistleblowing channel and the processing of reports. The provider is responsible for the technical implementation and maintenance of the channel. In addition, we may use office programs and other equivalent systems for the processing of personal data, with their maintenance and technical implementation conducted by the service provider. Our service providers process your personal data only in the capacity required to ensure the provision of the whistleblowing channel. We have data processing agreements with service providers who process the personal data, as required by data protection legislation.

5. Data transfers outside of the EU or the EEA

In principle, personal data is not transferred outside the EU or EEA.

In exceptional situations, service providers that participate in the production of the service may have access to the data system outside of the EU/EEA for purposes of providing technical support or service. In such cases, data transfers outside the EU/EEA to a nation for which the European Commission has not issued a resolution on the sufficiency of data protection are made in compliance with the EU Commission's standard contractual clauses and data protection measures. The data subject has the right to request more information on the transfer of personal data and applicable protection mechanisms.

6. Data security and data retention

System access is granted only to individuals who have the right to process data in connection with their duties, and these data processors are under the obligation of confidentiality. Each user has a unique user ID and password for accessing the system. The data is collected into databases that are secured with firewalls, passwords and other technical

means. The databases and any backup copies thereof are stored in locked facilities and accessible only to specifically designated individuals.

Data processors adhere to security procedures and employ processes to detect and prevent security breaches.

Data in the data file is retained for as long as is necessary to fulfil the purposes of processing or any legal obligations. As per the Whistleblower Act, the data is removed five years after the receipt of the report, unless it is necessary to retain the data for a longer period for the fulfilment of legal rights or obligations or for the establishment, exercise or defence of legal claim. More information on the retention periods and policies is available upon request.

7. Your rights as a data subject

As the data subject, you have the below rights, as per the General Data Protection Regulation and the Finnish Data Protection Act. However, these rights are not absolute – the execution and/or limitation of rights is regulated by law as well as any official regulations and guidelines that are not exhaustively described below. For instance, ARE may, in accordance with legislative requirements, have the right to limit the execution of below rights if such limitation is necessary and proportionate in terms of investigating the reports and securing follow-up actions or protecting the identity of the whistleblower. Any requests concerning the rights of data subjects should be submitted to the address specified in paragraph 1.

- **Right of inspection and right to demand rectification and erasure**
  - You are entitled to review your information stored in our personal data file and demand rectification or erasure of any erroneous data if there are legal grounds to do so.

- **Right to object and right to restriction of processing of data**
  - When the processing is based on legitimate interest, you have the right to object to the processing of your data on grounds relating to your particular situation and to request restriction of the processing of your data. Upon raising the objection, you must specify the particular situation on which you object to processing of your personal data. We may only refuse to honour the request by demonstrating compelling legitimate grounds to do so.
  - If the processing is based on our legal obligation, the right to object or to restrict the processing is not applicable.

- **Right to lodge a complaint with a supervisory authority**
  - You have the right to lodge a complaint with a supervisory authority, in particular in the EU Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of

personal data relating to you infringes the EU's General Data Protection Regulation. Contact information for the Finnish Data Protection Ombudsman is available here.

- **Information processed in the whistleblowing channel is never subject to automated decision-making.**

8. Contact information and privacy statement revisions

We kindly ask you to make all requests regarding this privacy statement in writing or in person in the address specified in the first (1) paragraph.

ARE may revise and update the privacy statement where necessary. Where required by applicable legislation, the revisions are reviewed with our employees. However, we recommend that you review this privacy statement from time to time.