WHISTLEBLOWING CHANNEL PRIVACY POLICY

Aspo Plc

1. GENERAL

This Privacy Policy describes how Aspo Plc ("Aspo" or the "Controller") processes personal data in connection with the whistleblowing channel. The Aspo Group consists of ESL Shipping Oy, Leipurin Oyj and Telko Oy. This Privacy Policy applies to all processing of personal data in relation to the whistleblowing reporting channel in all of the above-mentioned Aspo companies.

The reporting channel is an important tool for Aspo in monitoring potential misconduct and suspected violations. It enables rapid response and supports Aspo's employer and corporate image by providing a channel for raising concerns.

We comply with applicable data protection legislation in all processing of personal data. Data protection legislation refers to current data protection legislation, such as the European Union's General Data Protection Regulation (2016/679) and the Finnish Data Protection Act (5.12.2018/1050). Terms related to data protection that are not defined in this Privacy Policy shall be interpreted in accordance with data protection legislation.

"Personal data" means any information relating to a natural person ("data subject") from which that person can be directly or indirectly identified, as further defined in the GDPR.

2. DATA CONTROLLER AND CONTACT OFFICER

Data controller Aspo Plc
("Aspo")
Keilanranta 17 C 02151
P.O. Box 70
02151 Espoo
Tel. +358 9 5211

Contact person
Markus Riikonen/ Aspo Plc
Keilanranta 17 C 02151
P.O. Box 70
02151 Espoo
markus.riikonen (at) aspo.com

3. PURPOSES AND LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

Personal data are processed for the following purposes:

- Monitoring Aspo's operations
- Detecting, investigating and following up on crimes, breaches, misconduct or similar acts or omissions
- Developing, analyzing and compiling statistics related to monitoring
- Complying with statutory obligations

With the help of the whistleblowing channel, Aspo can monitor whether its organization complies with the rules and laws related to Aspo's decision-making and supervision system, especially in relation to money laundering, accounting, audits, corruption and bribery, environmental and economic crimes, competition law and violations of ethical guidelines.

The processing of personal data is based on the controller's statutory obligation to establish a whistleblowing channel for reporting misconduct and partly on the controller's legitimate interest in ensuring the ethical and lawful operations of the controller's employees and partners.

4. PERSONAL DATA AND SOURCES OF DATA PROCESSED

For the sake of clarity, it is stated that when using an anonymous whistleblowing channel, the whistleblower does not need to provide information about themselves that can be used to identify them.

The primary source of personal data is the online whistleblowing channel service, which allows anyone to submit reports of suspected misconduct to Aspo. Aspo strives to collect only such personal data that is necessary for the determination and investigation of the case. However, the extent of personal data submitted through the whistleblowing channel is determined at the whistleblower's discretion, which is why Aspo cannot always influence that it does not receive unnecessary personal data in connection with the report.

As a rule, the personal data processed in connection with the use of the whistleblowing channel is related to the whistleblower and the subject of the report. However, the report may also reveal the personal data of other persons, such as witnesses and colleagues, to the extent that the whistleblower has provided it to Aspo.

The whistleblower may provide Aspo with their basic information, such as their name, phone number and/or email address, through the whistleblowing channel or in some other way. However, the report can also be made anonymously.

Aspo processes the information that the whistleblower has provided to it about the person subject to the report, such as identification data containing the name and position of the person.

In addition, Aspo processes other personal data revealed in the report, for example, about the suspected target person and their actions that violate legislation or ethical principles. This information may also include personal data:

special categories of data, as well as personal data related to criminal convictions or offences.

After receiving the notification, Aspo will initiate an internal investigation into the matter, which will focus on assessing the conduct of the subject of the report and its compliance with the lawfulness or operating principles. In this context, Aspo also collects and/or generates personal data that may be related to all of the above-mentioned categories of data subjects and includes data belonging to all of the above-mentioned categories of personal data. The source of information can be a wide range of different parties, such as the original whistleblower, the personnel of Aspo and/or its group companies, and representatives of various stakeholders.

5. RETETION OF PERSONAL DATA

We store personal data for as long as is necessary to fulfil the purposes specified in this privacy policy or due to legal obligations. As a rule, the data included in the notification and collected during the investigation related to the notification are stored until the expiry of the time set for filing the claim. The retention period may also vary according to compelling legal requirements. As a rule, report data is stored for 120 days after the completion of the report related to the report, unless the storage of the data is necessary due to a criminal investigation, court proceeding or official investigation, or to safeguard the rights of the person who made the report or the person who is the subject of the report.

After the end of the purpose, the personal data will be deleted or anonymized within a reasonable period of time. Unwarranted reports containing personal data are immediately anonymised.

6. RECIPIENTS OF PERSONAL DATA

Aspo does not regularly disclose personal data to third parties. However, data may be disclosed to our group companies and in accordance with the law, for example to the police or other authorities for the purpose of investigating crimes. In addition, we may disclose information to the authorities when responding to requests for information from the authorities.

Aspo uses external service providers in the management of the whistleblowing channel and the processing of notifications. Personal data is transferred to external service providers only to the extent necessary for the implementation of the whistleblowing channel.

We ensure an adequate level of protection of our partners' personal data as required by law.

7. TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

Personal data will not be transferred outside the EU or EEA.

8. PROTECTION OF PERSONAL DATA

#

Data security and the protection of personal data are of paramount importance to us. The whistleblowing channel uses appropriate technical and organizational safeguards to protect personal data. The service provider of the whistleblowing channel processes personal data in secure server spaces. The service provider does not store IP addresses or other information that could be used to identify the sender of the notification. All reports in the whistleblowing channel are encrypted and can only be decrypted by designated people. The right of access to the information in the whistleblowing channel is restricted only to separately authorised parties. Parties processing personal data have a duty of confidentiality in matters related to the processing of personal data.

9. RIGHTS OF DATA SUBJECTS

Data subjects have rights to their personal data in accordance with data protection legislation. However, the application of the rights in each individual situation depends on the purpose and situation in which the personal data is used.

a. **The right to access personal data.** The data subject has the right to receive confirmation as to whether the data subject's personal data is being processed, as well as other information on the processing of personal data in accordance with

data protection legislation. The data subject has the right to receive a copy of the personal data. The right is exercised unless the law or some other applicable reason under data protection law requires us to deviate from this.

b. **Right to rectification of personal data.** The data subject has the right, subject to certain restrictions, to demand the correction or deletion of incorrect or inaccurate data.

c. **Right to erasure of personal data.** The data subject has the right to request the erasure of their personal data in accordance with the requirements of data protection legislation. Upon request, we will delete personal data, unless we are required or entitled to retain personal data by law or some other applicable exception in accordance with data protection legislation.

d. **Right to restriction of processing**. In accordance with the requirements of data protection legislation, the data subject has the right to obtain from Aspo the restriction of the processing of his or her personal data in certain situations.

e. **Right to object to processing**. The data subject has the right to object to the processing of personal data, including profiling, based on legitimate interests, in accordance with the requirements of data protection legislation. We may refuse a request if the processing is necessary for the purposes of the compelling and legitimate interests pursued by the controller or a third party.

10. EXERCISING RIGHTS

We hope that you will contact us if you have any questions regarding the processing of your personal data. You can send a request for data subject rights by letter or e-mail using the contact details provided in this privacy policy.

The applicant's identity will be verified before the request is processed. The request will be responded to within a reasonable time and, as a rule, within one month of the submission of the request and the verification of identity. If the request cannot be granted, the refusal will be notified separately.

11. RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

The data subject has the right to lodge a complaint with the competent data protection authority if the data subject considers that their personal data has been processed in violation of data protection legislation.

You can find the contact information of the Finnish Data Protection Authority here: Contact information of the Office of the Data Protection Ombudsman | Office of the Data Protection Ombudsman.

12. CHANGES TO THE PRIVACY POLICY

This privacy policy may need to be amended from time to time. The changes may also be based on changes in data protection legislation. We therefore recommend that you regularly review the privacy policy to detect changes. The latest version is available on our website.

This privacy policy was published on 3.2.2026.