

PROCEDURE FOR REPORTING MISCONDUCT

1 Introduction

- 1.1 The procedure for reporting misconduct (hereinafter referred to as the Procedure) describes **the reporting of misconduct** and/or circumstances that may harm people's health, the environment, the company's property or reputation (hereinafter referred to as misconduct) and the handling of relevant reports in Port of Tallinn group companies (hereinafter referred to collectively as the Port of Tallinn) principles and guidelines.
- 1.2 The main objectives of the procedure are:
 - 1.2.1 to support honest and ethical business activities and the Port of Tallinn's core values of "openness" and "reliability";
 - 1.2.2 encourage employees and third parties (partners, suppliers, customers, etc.) to report misconduct in order to prevent, detect, and solve problems at an early stage;
 - 1.2.3 to prevent and reduce any reputational and/or financial losses resulting from misconduct to both the Port of Tallinn and third parties.
- 1.3 All Port of Tallinn employees (including members of managerial bodies), representatives, and partners are expected to behave in accordance with high ethical standards, the principles of honesty and fairness in business operations, and legislation. The most important ethical principles presented to employees are described in the code of ethics of the Port of Tallinn and the procedure for avoiding conflicts of interest.
- 1.4 When reporting misconduct, the Port of Tallinn ensures:
 - 1.4.1 confidential and anonymous reporting;
 - 1.4.2 effective and independent reporting control;
 - 1.4.3 protection of the informant from potential retaliatory measures.
- 1.5 The key legal acts and internal documents related to this procedure are:
 - 1.5.1 EU Whistleblower Protection Directive¹;
 - 1.5.2 EU General Regulation on Personal Data Protection² and the Personal Data Protection Act³;
 - 1.5.3 The code of ethics;
 - 1.5.4 The procedure for avoiding conflict of interest;
 - 1.5.5 The procedure and principles of personal data processing.

2 Potential cases of misconduct

- 2.1 Workplace misconduct or inactivity includes, in particular (this list is not exhaustive):
 - 2.1.1 asking, offering or giving a bribe;
 - 2.1.2 fraud;
 - 2.1.3 decisions made in a conflict-of-interest situation;

¹ [23.10.2019 Directive 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law](#)

² [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#)

³ <https://www.riigiteataja.ee/en/eli/523012019001/consolidated>

- 2.1.4 damaging, wasting, or misappropriating the property of the Port of Tallinn or another person;
 - 2.1.5 violation of environmental requirements;
 - 2.1.6 violation of occupational safety or occupational health rules;
 - 2.1.7 violation of other legislation, the internal rule or procedure of the Port of Tallinn;
 - 2.1.8 discrimination or harassment;
 - 2.1.9 unethical behavior;
 - 2.1.10 other activities damaging the reputation of the Port of Tallinn.
- 2.2 Inactivity can also be classified as misconduct (e.g., the failure to comply with occupational safety requirements, or the failure to take a necessary decision in the interest of the Port of Tallinn in a conflict-of-interest situation).

3 Reporting channels for reporting misconduct

- 3.1 The Port of Tallinn expects to be notified of any misconduct if there are reasonable grounds to believe that a violation related to work-related activities has directly started or has been completed.
- 3.2 Misconduct can be reported internally in three ways: **publicly, confidentially or anonymously:**
- 3.2.1 In the case of public notification, the informant does not request confidentiality, and the relevant parties know who the informant is and what the notification consists of. It is easier to deal with public information and the risk of mistrust in the work environment is reduced.
 - 3.2.2 If it is not possible to report misconduct publicly, confidential reporting is an alternative. In the case of a confidential notification, the informant provides their name but expresses that their identity will not be disclosed during the inspection of the notification without their consent. Confidential notification provides the opportunity to contact the informant to clarify the circumstances or provide feedback.
 - 3.2.3 In the case of anonymous notification, the identity of the informant is not known, which can make it difficult to ascertain the circumstances of the misconduct and ensure protection for the informant.
- 3.3 **The reporting channels** for reporting misconduct are as follows:
- 3.3.1 the informant's immediate manager (in the case of the Port of Tallinn employee);
 - 3.3.2 the head of the internal audit department of the Port of Tallinn;
 - 3.3.3 through the Port of Tallinn's website (only in writing)⁴.
- 3.4 It is preferred that the informant first reports any misconduct they are aware of and tries to resolve the issue related to it by contacting their immediate manager (or their manager).
- 3.5 If the report concerns the immediate manager or there are other circumstances due to which it is not reasonable to expect the immediate manager to solve the problem, the notification can be submitted as follows:
- 3.5.1 confidentially, by informing the head of the internal audit department or another trusted individual who conveys the message to the head of the internal audit department;
 - 3.5.2 confidentially, by filling out the notification form on the website (appendix), leaving your contact information in the notification;
 - 3.5.3 anonymously, by filling out a notification form on the website without leaving contact details.⁵

⁴ The international [GlobaLeaks](#) platform is used as a notification channel.

⁵ To ensure complete anonymity, it is not recommended for an employee of the Port of Tallinn to use the computer of the Port of Tallinn for reporting.

- 3.6 When submitting a notification through the website, the system automatically generates a unique numerical code for the informant. This code allows the informant to later log in through the website to check if there is feedback or additional questions regarding the submitted notification. The code is not recoverable, so it is essential for the informant to securely retain the received code for tracking the subsequent processing of the notification, especially in cases of anonymous reporting where other means of communication are not available.

4 Receiving and handling reports

- 4.1 Receiving and checking notifications is organized by the internal audit department of the Port of Tallinn, which reports to the supervisory board of the Port of Tallinn for the purpose of ensuring independence and objectivity.
- 4.2 Notifications submitted to the head of the internal audit department and through the website are registered and handled confidentially within the scope of the Procedure by the individuals involved in their verification.
- 4.3 Notifications regarding the activities of employees in the internal audit department are not handled by the department under the Procedure; instead, they are forwarded to the chairman of the audit committee of the Port of Tallinn, who decides on further actions related to the notification.
- 4.4 Notifications made about the activities of a member of the supervisory board member of the Port of Tallinn, the chairman of the supervisory board of the Port of Tallinn will be informed (in the case of the chairman of the supervisory board, the chairman of the nomination committee of the Port of Tallinn is informed) , who decides on the future actions related to the notification.
- 4.5 Reports are primarily managed by the head of the internal audit department, and in their absence, the internal auditor takes over the responsibility.
- 4.6 The head of the internal audit department decides on the need to check the notification based on the information provided. **We do not verify notifications:**
- 4.6.1 that do not refer to the circumstances of professional misconduct specified in point 2 or of a similar nature;
 - 4.6.2 the data contained in it is not accurate enough to perform an investigation;
 - 4.6.3 in which a person, act, or entity is referred to impersonally.
- 4.7 The general handling process of reports is as follows:
- 4.7.1 the head of the internal audit department examines the content of the notification and decides the need and possibilities for its further inspection based on the circumstances presented in the report;
 - 4.7.2 the report is checked within a reasonable time according to the nature of the information contained in the notification, additional information is requested from the informant if necessary;
 - 4.7.3 feedback is given to the informant as soon as possible about the inspection results (if necessary, also the progress of the inspection) and the planned or implemented mitigation measures and improvement activities. In the case of an anonymous notification submitted via the website, feedback is provided via the online environment (the informant gains access using the unique code received when submitting the notification).
- 4.8 If necessary, the person under investigation is provided with an opportunity to provide their own explanations.
- 4.9 When the circumstances of a crime appear, the Port of Tallinn submits a report of a crime or misdemeanor to the police or other state authorities.

5 Ensuring confidentiality and protecting personal data

- 5.1 Notifications are treated confidentially to ensure adequate protection for both the informant and the person against whom the notification has been submitted. Depending on the content of the notification and its complexity, field experts or specialists may be involved, and the number of persons involved in handling the notification is kept as small as possible.
- 5.2 The identity of a confidential informant may be disclosed only with the consent of the informant. In the event that a threat to the informant's confidentiality emerges during the investigation of the circumstances of the informant and control activities, the head of the internal audit department will notify the informant.
- 5.3 When checking notifications, personal data is processed on the basis of legitimate interest and to a reasonable extent only for the purposes stated in the Procedure and for the protection of rights arising from the law, taking into account the procedure for processing personal data and the requirements of sectoral legislation.

6 Protection of the informant

- 6.1 Reporting misconduct, the Port of Tallinn ensures the informant's protection against possible pressure measures (also known as persecution)⁶. Harassment for providing notifications and assisting in these control activities is not permitted. If the informant sees a risk of applying pressure measures, it is advisable to contact the trustee, the head of the internal audit department, or your immediate manager to resolve the situation as soon as possible.
- 6.2 **Notifications that are groundless, malicious, or made for personal gain are not permitted.** The informant protection conditions are not guaranteed to a person who has repeatedly knowingly submitted incorrect information.

7 Notification register and reporting

- 7.1 The content of the notification, the most important notes related to the inspection of the notification, and the result are entered in the notification register kept by the internal audit department.
- 7.2 The head of the internal audit department provides the management of the Port of Tallinn (including the audit committee and/or the supervisory board) with a regular overview of the received notifications by topic, with regard to the most important notifications, an overview of the inspection results and implemented improvement activities is provided, taking into account confidentiality requirements.

⁶ Based on the EU directive on the protection of whistleblowers, Article 19 of which describes the use or threat of coercive measures (e.g. suspension of employment, dismissal, reduction of salary, disciplinary measures, etc.) as prohibited.

Appendix. Notification Form⁷

TALLINNA SADAM



TS Shipping

Tallinna Sadama grupi teavitusliin

Select the type of misconduct *

- Asking, offering or giving a bribe
- Fraud
- Decision taken in a situation of conflict of interest
- Damage, waste or misappropriation of property
- Violation of environmental requirements
- Violation of occupational safety or occupational health rules
- Discrimination or harassment
- Violation of legal requirements
- Violation of the company's internal rules or procedures
- Unethical behavior
- Reputational activity
- Other misconduct

The misconduct is related to the following company belonging to AS Tallinna Sadam group *

- AS Tallinna Sadam
- TS Laevad OÜ
- TS Shipping OÜ
- Can't answer

Where the misconduct occurred? *

Description of where the misconduct is known to have occurred (country, city/municipality, address, port, structural unit, etc.).

The time when the misconduct occurred? *

When the event took place (date and time). If the exact time is not known, then an approximate time or time period to the nearest year or month.

A detailed description of the misconduct *

A description of the content of the misconduct and all known circumstances, including a description of the action or inaction; related parties (names of persons, positions, persons external to the company); the negative impact of misconduct and estimated damage (including financial).

Is there written evidence of misconduct?

E.g. correspondence, documents, photos, videos, etc. in reproducible form.

- Yes
- No

Description of the origin of the information on which the notification is based

If there is no written evidence of misconduct, please describe the source of the information. If the information has reached you through other persons, please add their contact details.

⁷ The wording of the notification form may be supplemented in the online environment as needed.

Have you already reported the misconduct?

If you have reported, please name to whom you have reported the misconduct and whether it has been responded to accordingly.

If necessary, a description of other circumstances related to misconduct

I am submitting a notification

CONFIDENTIALLY, i.e. adding your contact information to the notification. They only reach the independent party analyzing the notification and may be necessary to request additional information. Your identity will not be disclosed at any stage of the process without your consent.

ANONYMOUSLY, i.e. the whistleblower's identity cannot be identified, which can make it difficult to explain the circumstances of the misconduct, and in this case we cannot guarantee you whistleblower protection measures.

Submit

In case of problems related to the submission of a notice, write to vihje@ts.ee

Powered by **GlobaLeaks**