

Rules of procedure

Protection of whistleblowers from violations of European Union (EU) law at work in HHLA TK Estonia AS

TABLE OF CONTENTS

1 Submission of information	1
2 Notification channel for reporting violations	2
3 Principles of the procedure	3
3.1 Confidentiality and data protection	3
3.2 Protection against repression and legal protection	3
3.3 Transparency and feedback	3

1 SUBMISSION OF INFORMATION

HHLA's business operations are based on honesty, fairness, respect, sustainability and transparency. HHLA's Whistleblower System is an important component of HHLA's compliance management system and aims to identify and address potential violations of law and internal guidelines within HHLA and its associated supply chains. Employees and relevant third parties and other stakeholders can report violations as part of the HHLA whistleblower system.

The Whistleblower System is designed primarily to receive information about potential violations within the HHLA Group or in its associated supply chains:

- Information about possible violations of applicable laws by HHLA Group employees (in particular violations of EU law under EU Directive 2019/1937 ("EU Whistleblower Directive"));
- Information about possible violations of internal company rules by HHLA Group employees (e.g. violations of the HHLA Code of Conduct or the HHLA Supplier Code of Conduct);
- Information about possible violations of human rights or environmental obligations under the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz ((Supply Chain Due Diligence Act), LkSG) within the business activities of HHLA itself or HHLA's direct or indirect suppliers;
- Information about potential human rights or environmental risks in accordance with LkSG within the business activities of HHLA itself or HHLA's direct or indirect suppliers.

2 NOTIFICATION CHANNEL FOR REPORTING VIOLATIONS

HHLA has established various channels for providing tips and information. HHLA's foreign subsidiaries have also published additional compliance contact addresses in case avoiders wish to contact only the relevant local compliance officer.

In particular, HHLA has created a digital HHLA Whistleblower Portal (BKMS® System) to identify and combat potential violations of the law and internal guidelines. It is available to all internal and external stakeholders who wish to report potential compliance risks and breaches digitally and anonymously (optional). Reports can be submitted at any time through a secure application provided by a dedicated service provider:

- HHLA whistleblower portal: <https://www.bkms-system.com/>

The HHLA Whistleblower Portal (BKMS® System) offers the whistleblower the opportunity to submit their report digitally and optionally anonymously and to communicate with the relevant subsidiary's local HHLA Compliance Officer or central HHLA Compliance Department without revealing their identity. Content is processed exclusively by HHLA's central compliance department and/or local compliance officers. Whistleblowers can decide whether and which contact details they wish to provide or whether they wish to remain anonymous. It is ensured that the whistleblower's identity is reliably protected and is not disclosed to HHLA or third parties if the whistleblower requests it.

Information can be provided through the following reporting channels:

Information can be provided to HHLA TK Estonia:

Email: compliance@hhl-tk.ee

Compliance Hotline: + 372 5300 8657

Mailing address: HHLA TK Estonia AS, compliance officer, Veose tn 16, 74115 Maardu city, Harju county

Personal meeting: Meetings are arranged through the aforementioned channel

Information can be provided to HHLA:

Email: compliance@hhl.de

Compliance Hotline: +49 40 3088 3777

Mailing address: Hamburger Hafen und Logistik Aktiengesellschaft, Group compliance officer, Bei St. Annen 1, 20457 Hamburg

3 PRINCIPLES OF THE PROCEDURE

3.1 CONFIDENTIALITY AND DATA PROTECTION

Reporting channels are designed so that the identities of whistleblowers - if they choose to remain anonymous - and third parties mentioned in the report are always confidential and unauthorized personnel cannot access this information. Employees of HHLA's Compliance Department are bound by confidentiality and impartiality. They will review the problem and, if necessary, conduct further investigation into the specific case.

The human rights officer, who is also located in the central compliance department, plays a central role in the process of reviewing potential violations.

As part of the Whistleblower System, HHLA processes personal data only in accordance with the applicable statutory data protection requirements, which are mainly contained in the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG). More information on data protection in the context of the HHLA whistleblower system can be found here: [Data protection information HHLA whistleblower system](#).

3.2 PROTECTION AGAINST REPRESSION AND LEGAL PROTECTION

Whistleblowers who report information in good faith are protected from adverse consequences and retaliation. Therefore, dishonest intentions arising from reports are not tolerated and are consistently held accountable. When clarifying information about violations, all parties involved are treated fairly.

3.3 TRANSPARENCY AND FEEDBACK

HHLA ensures that whistleblowers are adequately informed – provided that this is legally possible (in particular with regard to data protection legislation) – on further steps and actions after receiving information about potential breaches. As long as whistleblowers provide their contact information, receipt of information will be acknowledged within seven days of receipt. During the further process, whistleblowers have the opportunity to provide additional information about the matter in question and to contact the person responsible for reviewing the case as part of a joint discussion. The HHLA whistleblower portal (BKMS® System) offers the whistleblower the possibility of anonymous information exchange through a protected mailbox. During the procedure, in case of suspicion of a specific violation, it is ensured that appropriate corrective measures are taken to immediately eliminate the risks or violation, and measures are taken to prevent or avoid its recurrence. Whistleblowers will be duly informed of these planned or adopted follow-up measures – provided that this is legally possible (in particular in relation to data protection legislation) – within a reasonable period of time – a maximum of three months, or six months if the special circumstances require it. If the review of the case does not confirm the specific initial suspicions, the investigation will be stopped and the whistleblower will be notified in an appropriate manner.