Approved by RB Rail AS Management Board
Decision No 2/43/ 2019 on 5 August 2019

RB Rail AS
Whistleblowing Policy

Policy Holder: Security Risk Manager
Responsible division: CEO

History of versions

Version	Effective from	Comment	page
1	05.08.2019	Approved by MB decision No 2/43/2019 on 5 August 2019	

Content

1 Definitions

Company – RB Rail AS, reg. No 40103845025, including its branches - in Lithuania RB Rail AS Lietuvos filialas, reg. No 304430116, and Estonia RB Rail AS Eesti filial, reg. No 14168654.

Good faith - Good faith is evident when the Whistleblower report is made without malice or consideration of personal benefit and the Employee has a reasonable basis to believe that the Whistleblower report is true; however, it does not have to be proven to be true to be made in good faith.

Employee – Company's employee, applicant for employment, intern, secondee or former employee or any person engaged with the Company in an employment, contractual or similar type of relationship either currently or in past, including directors and managers;

Misconducts and Improper activities - Examples of misconduct include, but are not limited to, fraud, including financial fraud and accounting fraud, violation of laws and regulations, violation of Company policies, unethical behaviour or practices, endangerment to public health or safety, negligence of duty and other acts, which constitute infringement of laws or other regulations, which became known to the Whistleblower as part or in relation to his role as an Employee.

Policy – this Internal Whistleblowing Policy of the Company.

Whistleblower - A person making a protected disclosure about Misconducts and Improper activities in public interest and its Application is recognised as a Whistleblower report.

Whistleblowing – The act of reporting of Misconducts/Improper activities at the Company. It is an early warning system that enables the Company to find out when something is going wrong in time and to take necessary corrective actions to avoid harm to public interests.

Investigation – A process designed to gather and analyse information in order to determine whether Misconduct/Improper activity has occurred and if so, the party or parties responsible for that.

Informer – A person who submits an Application about Misconduct or Improper activities that might endanger public interests to the Security Risk Manager.

Application – an application submitted by an Informer according to Whistleblower reporting (Application) form regarding possible Misconduct or Improper activities taking place in the Company that might endanger public interests.

Whistleblower report – an Application that fulfil criteria set in the Policy to be recognized as a Whistleblower report by the Security Risk Manager.

2 Introduction

The Company conducts business based on the principles of **transparency, fairness, honesty, integrity and respect**, as mentioned by the Code of Ethics and Conduct and its corporate values – **people, professionalism, purpose** as stated in the RB Rail AS Mission Statement.

Together with the Company's values, the Company understands the importance of feedback and encourages Employees to speak up when they see activity or behaviour that they feel is wrong or does not match the Company's values.

The Company encourages its Employees to report about actual or suspected Misconducts and Improper activities

The goal of this Policy is to provide very clear guidelines on how the Company approaches and manages such feedback. The Policy addresses the Company's integrity and ethical behaviour by helping to foster and maintain an environment where Employees can act appropriately, without fear of retaliation. To maintain these standards, the Company **encourages** its Employees who have concerns about known or suspected Misconduct/Improper activity to **come forward and express these concerns without fear of punishment** or unfair treatment.

Members of staff or people connected to the Company may be the first to realize that a Misconduct or Improper activity endangering public safety is taking place at the Company. It is the Company's policy to support and encourage its Employees to report and disclose improper or illegal activities and to fully investigate such reports and disclosures.

The Company will address any justified complaints that allege acts or attempted acts of interference, reprisal, retaliation, threats, coercion or intimidation against Employees who report, disclose or investigate improper or illegal activities and will protect those who come forward to report such activities. The Company assures that all reports will be treated **strictly confidentially** and promptly dealt with.

Employees are encouraged to use guidance provided by this Policy for reporting all allegations of suspected Misconduct or Improper activity.

3 Commitment

The Company commits to ensure:

- every Employee has the chance to speak up when he/she feels the Company is not adhering to its corporate values or laws. There is a clear place to report misconduct, every Whistleblower report is heard and acted on, and the Company makes improvements based on the results;
- the Company protects informant's identity, and all reports are depersonalised prior to further processing;
- the Company will investigate every Whistleblower report of Misconduct or Improper activity. At the end of the investigation, the Company will document the results and provide feedback when appropriate.

4 Aims and scope

4.1 Aims of the Policy

- **To encourage** the Employees to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate;
- **To inform** the Management Board and Supervisory Board about acts of misconduct taking place at the Company;
- **To provide** to the Employees' guidance as to how to raise those concerns;
- **To reassure** Employees being protected from punishment for disclosing concerns in good faith and in accordance with this procedure;
- **To help** develop a culture of openness, accountability and integrity.

4.2 Scope of the Policy

Policy governs the reporting and investigation of improper or illegal activities at the Company, as well as the protection offered to the Whistleblowers who report about any kind of wrongdoing at the Company and whose Whistleblower report is in line with the rules set by the Policy. The Policy does not apply where the Application is made aiming to protect the personal interests of the Informer alone. Policy **applies to all Employees of the Company.**

The Policy applies to all Company's businesses, departments and branch offices. It also applies across all 3 Baltic states jurisdictions where the Company operates. If local legislation, regulation, or laws provide a higher level of protection than what is included in this Policy, the local legislation will take precedence.

Personal data of a Whistleblower, Whistleblower report, written or material evidence, and materials from the examination of the Whistleblower's report shall have the status of limited access information. Limited access information is managed in accordance with the RB Rail Regulation on Information Security Management.

4.3 Types of concerns covered by the Policy

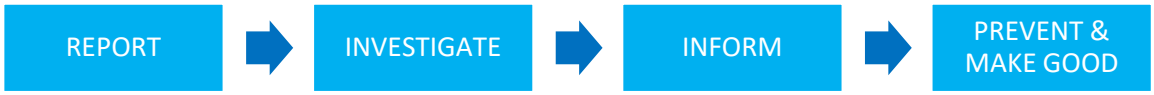
Policy applies if the Employee is reporting about any behaviour that endangers public interests and is:

- Fraudulent
- Illegal
- Corrupt
- Dishonest
- Unethical
- Is creating an unsafe environment
- Causing harm to the environment
- In breach of any of the Company's policies
- Discriminatory
- Financial malpractice or impropriety
- Harassment and/or bullying of any kind
- Detrimental to the Company and could cause financial or non-financial loss
- An attempt to cover up any of the above
- Other Misconduct/Improper activity

A whistle can be blown if the Employee has a reasonable suspicion that misconduct happening in the Company might endanger public interest.

5 Procedure

More detailed step by step whistleblowing procedure can be found in **Annex 2**.



5.1 General Guidance

Policy presumes that Informer **will act in good faith** and **will not make false accusations** when reporting of misconduct taking place in the Company. An Employee who knowingly or recklessly makes statements or disclosures that are not in good faith may be subject to disciplinary procedures. Employees who report acts of misconduct pursuant to this Policy can and will continue to be held to the Company's general job performance standards and adherence to the Company's policies and procedures.

Reporting in a bad faith may be subject to disciplinary proceedings

5.2 Confidentiality

All Whistleblower reports will be dealt with in strict confidentiality. Confidentiality will be maintained as far as possible in accordance with the need for an effective inquiry into the Whistleblower report. The identity of the Whistleblower will be protected.

5.3 Reporting of Misconduct or Improper activities

If a person has witnessed an Misconduct or Improper activity at the Company, that may adversely impact the public at large, he/she should report about it to the Security Risk Manager or in his/her absence to the General Counsel by e-mail: whistleblowing@railbaltica.org. Application should be submitted in English. Application can be submitted **by sending an email** or **notifying the** Security Risk Manager **in person**.

Although the Whistleblower is not expected to prove the truth of an allegation, he / she has to have a reasonable basis to believe that the information in the Whistleblower report is true

All Applications are encouraged to be sent by the email so as to assure a clear understanding of the issues raised. In case of Applications sent through email, it is recommended to mark the subject as '*Rail Baltica Whistleblower*' for ease of identification.

When Application is submitted in person, Informer and the Security Risk Manager together fill-in the Whistleblower reporting (Application) form and Informer signs it. In the Application, the Whistleblower:

- sets his/her name, surname.
- describes Misconduct or Improper activities that happened, are happening or will happen in the Company, where the person has serious ground to believe that the information provided is right.
- outlines specific facts, information about the natural or legal persons involved
- attaches evidence at the person's disposal in any form (e.g. photo, video, record, documents, correspondence, etc.).
- includes other information that is at the person's disposal and might be helpful during the investigation process.
- sign the Application.

For the whistleblowing purposes, the Whistleblower reporting (Application) form as provided in **Annex 1** should be used.

Anonymous Applications will not be treated as Whistleblower reports and such person's will only be protected in case and to the extent provided by the law

Informers are required to self-identify themselves and submit an Application containing all aforementioned information. It is one's duty to fill in the Whistleblower report (Application) form correctly otherwise Application will not be recognized as a Whistleblower report and Informer will not be recognized as a Whistleblower. In such case an Informer will not be entitled to the protection provided by the law. The Informer should provide all the information at his/her disposal, and that could help the investigation process.

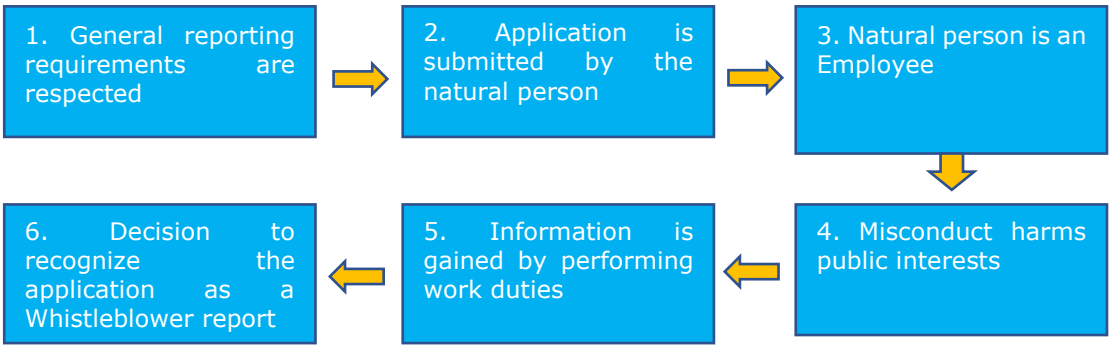
At any time, an Informer is suggested to consult with the Security Risk Manager on whether the situation noticed constitutes a Misconduct or Improper Activity. In case of any other ambiguities related to the whistleblowing,

Employee, Informer or Whistleblower can turn to Security Risk Manager or General Counsel (in case of the absence of Security Risk Manager) for clarification by sending an e-mail to whistleblowing@railbaltica.org.

5.4 Investigating Alleged Misconduct or Improper activities

The Security Risk Manager within seven days from the moment of receiving the Application shall depersonalize, and prima facie evaluate it and decide whether to recognize it as a Whistleblower report.

The Security Risk Manager checks, whether the **Application meet's the following criteria**:



After reviewing the Application prima facie, Security Risk Manager within three working days takes one of the following actions:

1. Recognize the Application as a Whistleblower report and notify the Whistleblower about the decision taken, or
2. Contact the Informer to clarify the uncertainties. When the Application does not meet the requirements set by the Policy fully, the Security Risk Manager can require the Informer to amend the Application and re-submit it, or
3. Not to recognize the Application as a Whistleblower report and notify the Informer about the decision taken. Informer can improve the Application and re-submit it again.

Within three working days after the Application is recognized as a Whistleblower report, the Security Risk Manager forwards it to the Whistleblower Committee and informs Management Board about the proceeding initiated, without revealing the identity of the Whistleblower.

If the Application is re-submitted by the same person, the Security Risk Manager forwards it directly to the Whistleblower Committee for revision. If the Whistleblower Committee considers the Application not meeting the requirements of a Whistleblowing report, the Committee can decide not to initiate the investigation. However, if the requirements set in the Policy are met, the Whistleblower Committee recognizes the Application received as a Whistleblower report and carries out the investigation.

5.5 Whistleblower Committee

After the Application is recognized as a Whistleblower report, the Security Risk Manager forwards depersonalized Whistleblower report to the Whistleblower Committee appointed by the Management Board.

Whistleblower Committee consists of the:

- Security Risk Manager
- General Counsel
- HR Manager
- Internal Auditor

The Whistleblower Committee is responsible for dealing with and settling reports made in the context of this Policy. General Counsel (in his absence – Internal Auditor) organises the work of the Whistleblower Committee.

If the Whistleblower report concerns a member of the Whistleblower Committee, then that member shall temporarily withdraw and will not be involved when the Whistleblower Committee deals with the Whistleblower report.

5.6 Investigation

Within five working days after receipt of a Whistleblower Report the Whistleblower Committee shall convene a meeting to discuss the action/investigation on the Whistleblower report.

The Whistleblower Committee has the responsibility to conduct investigations. To ensure an effective investigation, a member of the Whistleblower Committee is entitled to request information from any Employee. Information requested has to be provided in writing within seven working days from the day when the request of the information is received. The information has to be sent to the e-mail address specified by the member of the Whistleblower Committee or submitted directly to the member of the Whistleblower Committee in writing. The Whistleblower Committee ensures that investigations are carried out using appropriate channels, resources and expertise and can involve in the investigation also other Employees.

The investigation must be completed within a reasonable time frame but no later than within two months since the Application was recognized as a Whistleblower report. If it is not reasonably possible to complete the investigation within two months, the Security Risk Manager informs the Whistleblower that the Whistleblower Committee is still working on the case and the person will be notified when the investigation will be finished. In any case, the investigation should not take longer than three months.

5.7 After investigation proceeding

After the investigation is concluded and the Whistleblower Committee has passed the decision, Security Risk Manager informs the Management Board on the findings.

If the Whistleblower Committee has detected misconduct that might endanger public interest, then the Management Board takes the necessary decisions to eliminate problems identified by the Whistleblower Committee. The Management Board, in accordance with the national law (depending on the state), can impose disciplinary action against any Employee/-s who has violated the law or the Company's internal regulation and endangered public interests.

If the Whistleblower report concerns a member of the Company's Management or Supervisory Board or can significantly impact the Company's business, the Security Risk Manager presents findings of the Whistleblower Committee to the Chairman of the Supervisory Board. Supervisory Board in accordance with the national law (depending on the state) can impose disciplinary action against the member of the Management Board who has violated the law or the Company's internal regulation and endangered public interests.

The Security Risk Manager will keep the Whistleblower informed of the progress of any investigation and will notify the Whistleblower on completion of the investigation. Security Risk Manager will also inform the Whistleblower of what action, if any, is to be taken bearing in mind that the need for confidentiality may prevent disclosure of specific details of the investigation or any disciplinary action taken as a result. Any information given by the Security Risk Manager to the Whistleblower will be regarded by them as strictly confidential and may not be disclosed to third parties except with the express consent of the Security Risk Manager. The Whistleblower does not have the right to access or to examine the full findings.

The Security Risk Manager monitors compliance with the sanctions or follow-up actions that have been taken.

6 Rights of the Persons involved

6.1 Informing interested parties about the Whistleblower report

Employees about whom a Whistleblower report is received shall be informed about the procedure, his/her rights and the persons/departments who might receive the Whistleblower report. The Employee will be offered the opportunity to give his/her view on the Whistleblower report.

However, if there is a risk that such notification to the alleged person would jeopardize the ability to investigate the Whistleblower report effectively, the notification can be delayed as long as necessary for an effective investigation.

Under no circumstances can an Employee about whom the Whistleblower report is received, obtain information about the identity of the Whistleblower, except where the Whistleblower maliciously makes a false statement.

The Whistleblower's identity is anonymized by the Security Risk Manager and the name of the person will not be disclosed to anyone

If the Whistleblower Committee concludes that the Whistleblower has made a false statement it informs the Security Risk Manager accordingly. Security Risk Manager reveals the identity of the Whistleblower to the Management Board, which takes the decision on further action. In such cases the Employee who used internal whistleblowing mechanism in bad faith might face the disciplinary sanctions.

6.2 Protection of the Whistleblower

The Whistleblower is protected by the law and retaliation against it will not be tolerated

The Company guarantees that a **Whistleblower report** made in a good faith and about a (possible) infringement or malpractice will not have any consequences for the employment-law position of the Whistleblower, that this will not have any effect on the Whistleblower's remuneration, and that this **will not have a negative impact on the Whistleblower's** performance reviews.

Under no circumstances may a member of the Company's staff **retaliate against a Whistleblower**. If a member of staff is involved in such conduct, they may be subject to a disciplinary action.

The Company aims to encourage openness and supports Employees who raise genuine concerns under the Policy, even if the information provided by the Informant turns out to be mistaken. However, before submitting the Application, Informant should have a **reasonable belief** that the **information** provided **is correct** and actually **endangers public interests**. If during the investigation proceeding turns out that the information provided is incorrect, but the Informant had reasons to believe that it is correct, Informer is not retaliated.

6.3 External disclosure

The aim of the Policy is to provide an internal mechanism for reporting, investigating and remedying wrongdoing at the Company. In most cases therefore an individual should not find it necessary to alert anyone externally to their concern.

Latvian State Chancellery, Lithuanian Prosecutor's office are the contact points for the Whistleblowers reporting externally

The law recognizes that in some circumstances it may be appropriate or required for an individual to report their concerns to an external body like competent authority or association, foundation, trade union or other kinds of establishment. In case of any question regarding whistleblowing, a person can contact the **Whistleblower contact point** by an email Inese.Kuske@mk.gov.lv or phone number: +371 67082910. In case a person wants to submit a Whistleblower report to State Chancellery it can use an email trauksme@mk.gov.lv , phone number +371 67082837. More information about the Whistleblower contact point can be found on the Latvian State Chancellery official website: https://www.mk.gov.lv/lv/content/trauksmes-celeji (available only in Latvian) and Latvian State Chancellery contact information is available at https://trauksmescelejs.lv/kontakti. In case of Lithuanian Branch of the Company, the Lithuanian Prosecutor's Office is the institution, whereby external Whistleblower reports are to be made in the cases prescribed by law.

It will rarely, if ever, be appropriate to inform the media.

Disclosing information publicly should be the last step taken, only when other whistleblowing channels turn out to be ineffective

For Latvia and Estonia: only if the internal whistleblowing system turns out to be ineffective (there is no response to the applications received, no action taken to eliminate the threat to public interests, external whistleblowing channels are ineffective as well) only then person can disclose the information publicly. However, no person is allowed to publicly disclose information classified as state secret. Before reporting a concern externally, the Company strongly advises any individual to seek an advice.

For Lithuania: Misconduct/Improper activity may be reported publicly in case of a threat to human life, public health or the environment, where urgent action is needed to prevent such a threat and there is no other way to report the misconduct/improper activity due to a lack of time or no timely action was taken upon making notification by other means. In order to obtain the statutory protection, the Whistleblower shall contact the Lithuanian prosecutor's office.

7 Administration of the Policy

7.1 Summary

The received Whistleblower report, written evidence, and materials from the examination of the Whistleblower's report shall be registered in the Company's Document Management System, indicating the relevant document classification level, related file number in record-keeping and storage period, but the document is not placed in the Document Management System. The folder location is as follows:

RB Rail AS › RailBaltica Intranet - Documents › RB Rail › Whistleblowing

The Whistleblower case documents in paper form and material evidence shall be stored separately in lockable cabinet or safe, but electronical documents in the Company's Information System at the same time ensuring

that the documents are protected and available to specific users only (Security Risk Manager and Whistleblowing Committee members).

By 15 January each year the Security Risk Manager summarises all the Whistleblower reports received in the previous calendar year. Summary and main findings are presented to the Management Board of the Company and the Internal Auditor. The summary will not contain details on the reported issue nor the identity of persons mentioned in the Whistleblower report, or the identity of the Whistleblower.

Latvian State Chancellery on a yearly bases collects information about whistleblowing and protection of the Whistleblowers. Upon the call of the Latvian State Chancellery, the Company can provide a summary of the Whistleblower reports received and other information that State Chancellery specifies, without revealing the identity of the Whistleblowers.

7.2 Data retention

Personal data processed in a Whistleblower report shall be dealt with in accordance with the Company's Privacy Policy and kept for the period of the investigation. If no investigation is initiated, the Application is kept for a period of one year since the decision taken on not to recognize Application as a Whistleblower report. If an investigation is commenced the Whistleblower report and information gained during the investigation period is kept for a period of five years from conclusion of the investigation.

7.3 Review of the Policy

From time to time, the Company's Policy will be amended to keep up with the Company's values, best practices, improvements, as well as legislation and regulations. The recommended review period is two years.

Any amendments to the Policy will be communicated with Employees and any relevant stakeholders.

The Management Board will review all amendments, and the Management Board can comment and provide feedback as necessary and approved by the Company's Supervisory Board.

7.4 Availability

The Policy is available to all Employees online together with other Company's policies.

The Policy is based on the Latvian Whistleblowing law and is in line with the mandatory laws of Estonia and Lithuania.

Annex 1

WHISTLEBLOWER REPORT (APPLICATION) FORM

Please provide the following **details for any suspected misconduct** to any breach or suspected breach of the law or regulation that may adversely **impact the Company and public interests**. Please note that you may be called upon to assist in the investigation, if required.

Completed Whistleblower report (Application) should be submitted to the Security Risk Manager or in case of his/her absence to the General Counsel by e-mail: whistleblowing@railbaltica.org.

Note: Please follow the guidelines as laid out in the Internal Whistleblowing Policy.

To: Security Risk Manager of RB Rail

1. Details of concerns:
Please provide available details, such as names, dates and places and the reasons for the concerns (continue on separate sheet if necessary) together with any available supporting evidence (like documents, photography, email correspondence etc.).
2. Way of obtaining information (in relation with the work duties)
Your relationship with the organization where the alleged violation has been observed (tick as appropriate): ☐ I am working at the Company (contractual relationship) ☐ I am a former employee of the Company ☐ I am/was an intern of the Company ☐ I noticed possible violation of the rules while establishing a contractual relationship ☐ Other (please specify) _____
3. Please indicate what **public interests are endangered**[1] by the wrongdoing you have noticed (optional)
4. Annex
Specify the documents (if any) attached to the Application that you believe confirm the alleged infringement.

[1] Reporting of personal interests only is not considered as a whistleblowing

1. 2. 3.
6. Details of the Informer
Name: _____ Address: _____ Tel No: _____ Email: _____ Date: _____
Personal Information Collection Statement All personal data collected will only be used for purposes which are directly related to the whistleblowing case you reported. The personal data submitted will be held and kept confidential by RB Rail in accordance with the Privacy Policy of RB Rail AS.

By submitting this Application, I:

- agree to the processing of my personal data (registration of the Application, verification of the specified information and reconnection with me) in line with the Privacy Policy of RB Rail AS;
- certify that I have reasonable basis to believe that the information contained in my Application is true;
- am aware that I may be held responsible for deliberately providing false information.

This Application will be reviewed by the Security Risk Manager (or in case of his/her absence by the General Counsel) who will decide whether this Application can be recognized as a Whistleblower report according to the criteria set out in the RB Rail Internal Whistleblowing Policy. If your Application is not recognized as a Whistleblower report, please choose your preferred course of further action regarding your Application:

A. I agree that my Application will be considered as an ordinary private individual's application (meaning, I have no identity or security guarantees of a Whistleblower)

☐

OR

B. I recall my Application and all data in relation to it is permanently deleted by the Company

☐

_____ (signature)

To be completed by the institution / organization

Application Registration Date _____ No _____

Information on the further communication - Within three days of the decision to recognize your Application as a Whistleblower report, you will receive a response on the decision taken (using the contact details provided in paragraph 6 of this application); - If necessary, you may be contacted for further information; - If your Application is recognized as a Whistleblower report, the Security Risk Manager will inform you of the progress of its investigation within two months of the date of acknowledgment of your application as an alert;

- In case of uncertainties, you can contact the Security Risk Manager at any time.

WHISTLEBLOWING PROCEDURE

Annex 2 WHISTLEBLOWING PROCEDURE
In force since

Rail Baltica