

AS Piletilevi Group
BREACH REPORTING PROCEDURE

1. INTRODUCTION

Breach Reporting Procedure (hereinafter **Procedure**) of Piletilevi Group AS (hereinafter **Piletilevi** or **we**) provides for the procedure for submitting and processing reports of breaches concerning the Piletilevi Group and the protection of reporting persons from retaliatory measures.

Piletilevi ensures a safe environment in which to report misconduct. The procedure sets out a framework and guidelines under which any misconduct can be reported.

This procedure is based on the Act on Protection of Persons Who Report Work-Related Breaches of European Union Law and the General Data Protection Regulation. The current procedure can be found electronically.

2. IMPORTANT TERMS

- **Reporting person** – a person who reports a potential threat or breach.
- **External reporting** – providing information about the breach to the competent authority.
- **Disclosure to the public** – making information about the breach or omission available to the public.
- **Work-related context** – current or previous work-related activity, in any sector and field, regardless of the nature of the work-related activity, through which the reporting person receives information about the breach.
- **Competent authority** – a state authority or EU body competent to receive a notification of a breach and to process the reported breach.

3. BREACH

3.1. Meaning of breach

By breaches, including potential breaches, we primarily mean misconduct where Piletilevi employees, partners or other related parties are in breach of applicable laws or where their actions are not in breach of the requirements of the law, but are contrary to the purpose of the law or the internal rules of Piletilevi (hereinafter referred to as **breach** or **work-related misconduct**).

3.2. Who can report a breach?

The procedure applies and internal reporting is intended for all Piletilevi employees, members of management and all other persons providing services to Piletilevi, regardless of their position or status.

3.3. What types of breaches can be reported?

The procedure of reporting a breach applies to the following areas: public procurement, competition law, corruption, accounting, financial and tax law, environmental protection requirements, etc. However, the procedure of reporting a breach is not intended to resolve consumer and labor disputes.

Please note that you can also report other work-related breaches that are not related to European Union law. However, the person reporting a work-related breach must have reasonable grounds to believe that the breach has been immediately initiated or completed and that the information provided is true. It is prohibited to submit a knowingly incorrect breach report.

This procedure does not apply to personal disputes, such as bullying, harassment, discrimination and other similar cases, unless it is a case of public importance. Therefore, a dispute arising from bullying employees at work or any other dispute between employees is not a work-related breach.

Some examples of breaches:

- The company uses customers' personal data without consent, for example for targeted advertising or shares it with other companies.
- The company knowingly uses misleading pricing strategies, such as adding hidden fees during the ticket purchase process that are not clearly disclosed in advance.
- The company intentionally misrepresents financial statements to avoid taxes.

4. REPORTING OF A BREACH

4.1. Reporting to Piletilevi

In Piletilevi, it is possible to report work-related breaches by e-mail at whistleblower@piletilevigroup.com (hereinafter referred to **as internal reporting channel**).

When reporting a breach to the internal reporting channel, please provide the information described below:

- the name of the reporting person;
- the personal identification code or date of birth (optional) of the reporting person;
- the contact details (personal email address and contact telephone number, if possible) of the reporting person;
- the position or collaborative relationship of the reporting person;
- if you are reporting at the request or on behalf of another person, the name of that person;
- the time and place of the breach;
- description of the breach;
- persons involved in the commission of the breach;
- who you have informed about the breach and what consequences it entailed;
- who else is aware of the breach;
- an indication if confirmation of receipt of the breach report and information on the implementation of follow-up measures and the final outcome of the procedure are not expected to the published contacts;
- a confirmation that, in the opinion of the reporting person, the information provided, and the statements contained therein are true and that the reporting person has not knowingly submitted a false report and published incorrect information.
- The information specified in points 1-3 (i.e. the name, personal identification code/date of birth, contact details of the reporting person) does not need to be provided if the reporting person wishes to remain anonymous.

4.2. Other ways to report a breach

If the internal reporting channel provided for in these procedures is not suitable for the reporting person, the breach report may also be submitted to another competent authority through an external reporting channel established by them. For example, it is possible to report violations related to consumer protection to the Consumer Protection and Technical Regulatory Authority according to the procedure published on their websites.

In addition, it is possible to disclose a work-related breach to the public. It is also possible to publicly notify the public of a breach if the breach may cause a risk of harm to the public interest or if circumstances do not allow the breach to be resolved through an external reporting channel.

4.3. Prohibition of submitting an incorrect breach report

The reporting person must act in good faith and with reasonable grounds to believe that the information provided, and the allegations contained therein are true. It is prohibited to submit a knowingly incorrect breach report.

4.4. Anonymous reporting of a breach

- It is also possible to report a work-related breach anonymously.
- However, we would like to point out that in the case of anonymous reporting, anonymous reporting persons do not enjoy the rights and protections provided for in applicable law. Also, in the event of an anonymously submitted breach report, no notification or feedback will be provided to the reporting person regarding the processing of the breach report.

5. PROCESSING OF A BREACH REPORT

5.1. General information

The persons processing the reports are divided as follows:

- Hanna Jõgis, Chief Customer Success Officer, handles the processing of customer-related breaches.
- Kadri Otspere, Group Chief Human Resource Officer, handles the processing of personnel-related violations.

The handlers are responsible:

- for receiving breach reports;
- for maintaining contact with the reporting person and providing feedback and, if necessary, requesting additional information;
- for informing about the implementation of follow-up measures.

5.2. Receiving a breach report

- If the reporting person sends a breach report via the internal reporting channel, Piletilevi will confirm receipt and verification of the report within seven days (except in the case of anonymous reporting).
- If there is no competence to process the breach report, the notification shall be forwarded to the competent authority immediately, but no later than the fifth working day after receipt of the breach report, and the reporting person shall be notified thereof at the same time.
- Breach reports are processed in Estonian and English.

5.3. Careful processing of the breach report

- After receiving a breach report, Piletilevi will immediately begin processing the breach.
- The confidentiality and protection of the reporting person will be ensured during the investigation.
- If necessary, the reporting person may be asked for additional information and evidence.

5.4. Feedback to reporting

- The reporting person will be provided with feedback no later than three months after receipt of the breach report.
- If the investigation takes longer, the reporting person will be provided with regular feedback on the procedure.
- Notifications will not be sent to the reporting person if the report has been submitted anonymously or if the reporting person has expressly prohibited the sending of information or there is reason to believe that this would jeopardize the reporting person's confidentiality.
- If, based on the information provided in the breach report, there is a suspicion that an offense has been committed or is planned to be committed, a crime report may be filed with the prosecutor's office and the police, in addition to other legal measures.
- In the interests of a potential or ongoing investigation, the reporting person may in certain cases be required not to disclose information about the reporting, investigation, or progress of the breach.

5.5. Resolution of the breach

- If the investigation shows that a breach has occurred, measures must be taken immediately to remedy the situation and end the breach. If the investigation determines that a breach has occurred, Piletilevi must implement appropriate measures to end the breach and prevent future occurrences of the breach.

6. ENSURING THE PROTECTION OF THE REPORTING PERSON

- We assure you that the reporting person will be treated with the utmost confidentiality and protected from any retaliation or discrimination that may result from reporting a breach.
- No retaliatory measures will be taken against the reporting person (e.g. reduction of salary or work benefits, demotion, dismissal, etc.).
- The dissemination of confidential information to third parties without reason must be prevented. If dissemination occurs, efforts must be made to stop the spread of information and to identify the source and extent of the leak.
- The identity of the reporting person may only be disclosed with the written consent of the reporting person. If criminal or misdemeanor proceedings are initiated based on a breach

report, the confidentiality of the fact of the reporting is ensured by the specifications provided for in the relevant procedural code.

- When reporting a breach, we always assume good faith until proven otherwise. The protection of the reporting person does not cease if the reporting person has submitted an incorrect report in good faith.
- If the reporting person later discovers that the information published is untrue, they may still benefit from the protection offered to reporting persons, if they have reported this new information in a timely manner.

7. PROHIBITION OF RETALIATION

- The reporting person is protected from discrimination or other negative consequences in connection with the breach report.
- If it is determined that Piletilevi has used retaliation or harassment against the reporting person, made a corresponding attempt, or threatened to use retaliation, the case will be investigated and, if necessary, measures will be taken to eliminate the retaliation.
- An employee involved in the retaliation is liable for their actions in accordance with the procedure prescribed by law.
- Reporting persons who believe they have been the victim of retaliation or have good reason to believe they are at risk of retaliation should immediately report this to the person handling the breach.

8. INFORMATION ON THE PROCESSING AND STORAGE OF PERSONAL DATA

- Piletilevi processes all personal data in accordance with applicable law, including the requirements of the Act on Protection of Persons Who Report Work-Related Breaches of European Union Law and the General Data Protection Regulation.
- All breach reports and related documentation are stored by Piletilevi for three years from the date of feedback on the breach report in a separate folder with limited access, which is managed by the HR manager.

9. SUMMARY

- These procedures are updated regularly to ensure compliance with applicable law, including the Act on Protection of Persons Who Report Work-Related Breaches of European Union Law.
- For questions regarding the breach reporting procedure or to report a work-related breach, please contact Piletilevi using the details below:

AS Piletilevi Group

whistleblower@piletilevigroup.com

