

4.10.2024

PRIVACY POLICY

Controller

Tornator Oyj, Einonkatu 6, 55100 IMATRA

Contact person responsible for the register

tuija.luukkanen@tornator.fi

Name of the register

Personal data register of the whistleblower system

Purpose and legal basis for processing personal data

The whistleblowing channel has been created to report suspected misconduct, such as money laundering, tax evasion, environmental violations or other illegal activities. Through the channel, it is possible to report actual or potential crimes, violations, abuses and negligence that violate EU regulations as defined in Directive (EU) 2019/1937. With the help of the whistleblowing channel, the organization can receive information about suspected misconduct and react to it in time, as well as take the necessary measures to prevent similar situations in the future. The legal basis for the processing is compliance with Tornator Oyj's legal obligations.

- **Receiving and processing reports:** The system allows employees and other stakeholders to report suspected misconduct or illegal activity. The processing of personal data is necessary in order to investigate the reports and to take any measures.
- **Investigation and investigation of misconduct:** Personal data is processed as part of the investigation and investigation of reports, including information on potential suspects and related persons.
- **Safeguarding the rights of workers and others:** The system ensures that the rights of whistleblowers are protected and abuses are addressed where necessary.
- **Compliance with laws and regulations:** Personal data is processed to fulfil the organisation's obligations, for example in accordance with the EU Whistleblower Directive (2019/1937) and data protection legislation (GDPR).

Personal data processed and data collection

The whistleblowing channel may contain personal data on both the whistleblower and the persons targeted by the report, including those persons who, based on the report, are found to be linked to suspected misconduct.

The notifier can provide their own names and contact details if they wish. Identification data, information on suspected violations of the law or ethical guidelines, and other information provided by the whistleblower are processed about the subjects of the report. In addition, information on the events related to the report, possible misconduct, related measures and sanctions is processed. Other information may also come to light during the investigation, especially in relation to the assessment of the legality of the actions of the target persons or their compliance with the Code of Conduct. Reports of misconduct can be made through the Whistleblower form on Tornator Oyj's website.

Retention period of personal data

Personal data will only be stored for as long as necessary to achieve the purposes specified in this policy. Information that is not essential to the processing of the report will be deleted as soon as it becomes unnecessary. The stored personal data will be deleted no later than two years after receipt of the notification, unless the retention of the data is necessary, for example, due to legal proceedings or other measures, and if an appeal is no longer possible. In such cases, the data will be retained for the necessary period of time to take legal action or to prepare, exercise or defend legal claims.

Disclosure of personal data to third parties

The data will not be disclosed outside the controller and the channel's technical service provider. As an exception to this, the data subject's personal data may be disclosed to authorities, such as the police, in situations where the controller has a legal obligation to report a violation and in situations where there is cooperation with the authorities based on law.

Principles of register protection

We have put in place appropriate physical, technical, and managerial measures to protect personal information from loss, destruction, misuse, and unauthorized access and disclosure. The controller has predetermined which of the employees have the right to process the data in the whistleblowing channel based on their work duties and position. Only these people have access to the system and use personal credentials, as well as passwords that are changed regularly, as well as two-factor authentication. Everyone who processes personal data is bound by professional secrecy, and everyone is trained to comply with privacy policies. Personal data is disclosed to third parties only to the extent necessary to investigate the case. The identity of the whistleblower is kept confidential as far as possible if it is possible for the investigation of the report.

The whistleblowing channel and related information systems are protected by technical means to prevent the destruction, loss, alteration or unauthorized disclosure of information. While we have implemented all reasonable security measures, it is important to note that no system can completely eliminate the possibility of security risks. In the event of a potential data breach, we will inform you of the situation as required by law.

Rights of the data subject

A person has the right to view personal data concerning them if it does not jeopardise the anonymity of the whistleblower or the processing and investigation of the report through the Whistleblowing reporting channel. The data subject's right to see their own data may be restricted when it is necessary to protect the investigation or to safeguard the identity of the whistleblower. The data subject also has the right to request the rectification of incorrect or inaccurate data. Requests for rectification are carefully examined, and if no consensus is reached, the data subject's perspective can be added to the information. The original information is stored along with the corrected information. Data may be deleted upon request, provided that there are no legal or purpose-related obstacles to the deletion. All deletion requests are carefully reviewed and, if the data cannot be deleted, the requestor is given a clear justification. The data subject may request the restriction of the processing of his or her personal data, and each request will be assessed on a case-by-case basis based on its appropriateness.

In relation to the whistleblowing system, the controller has the right to restrict the data protection rights of the person subject to the report. Restriction of rights may be necessary, for example, when it is necessary to avoid hindering or slowing down the processing of reports, preventing the verification of the accuracy of reports, or seeking to protect the identity of the whistleblower. The restrictions are in force only for as long as it is necessary for the investigation.

Data subjects can exercise their rights by sending their request to tietosuoja@tornator.fi. If the data subject feels that there are deficiencies in the processing of personal data, he or she has the right to contact the Office of the Data Protection Ombudsman. Contact information can be found here: <https://tietosuoja.fi/etusivu>.