

Data Privacy Notice for Whistleblower-channel

This privacy notice concerns the collection and processing of personal data through Temet Whistleblower-channel.

1. Data Controller

The entity responsible for the processing of personal data as referred to in this privacy notice is as follows:

Temet Group Oy (Business ID 3108487-6)

Hannuksenpelto 3, 02270 Espoo

Phone: 0207 600 700

2. Purposes and Legal Bases for Processing Personal Data

Reports of observed violations and misconduct are made through the reporting channel. The report may contain personal data if the reporter includes them in the report. Personal data is processed solely for the purpose of fulfilling the statutory obligations of Temet Group Oy and its subsidiaries (hereinafter "Temet") and processing the received reports, as well as for the exercise of supervisory and control rights.

Processing is based on the statutory obligation of the data controller or the legitimate interest of the data controller or a third party concerning the personal data of third parties, such as the information of individuals subject to the report, and the consent of the reporter or the legitimate interest of the data controller or a third party concerning the information of the reporter. Regarding the personal data of individuals processing the reports, the processing is based on a statutory obligation or legitimate interest.

Reports received by Temet are handled by individuals appointed by Temet Group for the processing of reports. Personal data included in the report may be used to investigate the reported matter.

3. Data sources of personal data

The reporter provides information about observed misconduct or violations. By default, the report does not contain personal data about the reporter unless expressly provided by the reporter. If the reporter provides personal information about themselves, they are treated as data subjects.

The report may also contain personal data about individuals other than the reporter if the reporter deems them necessary for making the report. These may include, for example, photographs, videos, or texts.

Personal data may also be collected in connection with the processing of the report. Necessary information about the handlers of reports is collected for the processing and access control of reports.

Collected personal data may include, among other things, name, phone number, email, position, and, if necessary, the role as a data processor. The reporting channel itself does not collect information enabling the identification of the reporter, such as IP addresses or cookie data.

4. Processing of Personal Data

Personal data are processed to handle the reports received through the reporting channel. Based on the reports, the data controller takes necessary actions.

Personal data contained in the report are stored securely in the database of the reporting channel service. The data are accessible only to the designated handlers of reports appointed by the data controller. The data controller may restrict access to reports based on different types of reports or the role of handlers. If necessary, the data controller may transfer the data to its own database for processing or archiving. Data is stored securely.

5. Disclosure of Personal Data

Personal data are processed by the designated handlers of reports appointed by the data controller. Handlers do not disclose personal data to third parties except in situations based on law, such as if the processing of the report leads to an official investigation or if disclosure is necessary to implement measures required by the investigation of the report's findings.

Personal data may also be shared with third parties in situations where the impartiality of the processing of reports cannot be guaranteed due to the affiliations of the handlers appointed by the data controller. In such cases, to ensure the impartial processing of the report, the data controller may authorize an external handler/handlers to process the report in accordance with this notice and legal requirements. Such an external handler may be, for example, an HR professional, auditor, lawyer, or other independent expert.

6. Transfer of Data Outside the EU Area

Personal data are not transferred outside the EU area.

7. Security of Processing Personal Data

Temet reporting channel is implemented within the First Whistle system by Juuriharja Consulting Group Oy.

Only the handlers of reports appointed by the data controller are informed of the reports and have access to process the reports in the service. Each handler uses their individualized user credentials to log in and process the reports. If a report concerns one of the handlers, they are excluded from handling the report.

Reports and related information are archived securely. Designated handlers of reports have access to archived information.

8. Data Retention Period

Unless otherwise required by mandatory legislation, data are retained as long as necessary for the investigation of the report or the processing of the matter.

However, data are deleted 2 months after the closure of the report or at the latest two years after the implementation of the consequences determined based on the investigation, unless further retention is necessary for the enforcement of rights or obligations prescribed in this or other legislation, or for the establishment, presentation, or defence of a legal claim. Personal data that clearly have no significance for the processing of the report are deleted without undue delay.

9. Rights of the Data Subject

The data subject has the following rights:

- **Access right.** The data subject has the right to obtain confirmation from the data controller whether personal data concerning them are being processed and to access the personal data we have stored. Personal data can be accessed by requesting the information via email at tietosuoja@temet.com.
- **Right to rectification.** The data subject can request the correction of inaccurate or incomplete information concerning them.
- **Right to restriction.** The data subject can request us to restrict the processing of their personal data if they believe that their personal data have been processed unlawfully or if the data subject disputes the accuracy of their personal data.
- **Right to object.** The data subject has the right to object at any time to the use of their data for direct marketing purposes. We will process the data subject's request to object to the use of their personal data for purposes other than direct marketing, after which we will either cease processing the personal data or provide a justified reason for continuing the processing of the data.

- **Right to erasure.** The data subject has the right to request the deletion of data if the processing of the data is not necessary. We will process the deletion request, after which we will either delete the data or provide a justified reason for not being able to delete the data.
- **Right to data portability.** The data subject has the right to receive the personal data concerning them, which they have provided to the data controller, in a structured, commonly used, and machine-readable format, and the right to transmit those data to another controller if the processing is based on consent or a contract between the data controller and the data subject, and the processing is carried out by automated means. We will process the request for transfer, after which we will either transfer the data or provide a justified reason for not being able to transfer the data.
- **Right to lodge a complaint.** The data subject has the right to lodge a complaint with a supervisory authority if he/she considers that the processing of personal data breaches his/her rights pursuant to applicable law. Office of the Data Protection Ombudsman <https://tietosuoja.fi/en/contact-information>

10. Automated Decision Making or Profiling

There is no profiling or automated decision-making related to the personal data and their processing concerning the reporting channel.