

Privacy statement | SATO's Whistleblowing channel

1. File controller

SATO Corporation, Panuntie 4, PO Box 401, 00601 Helsinki, phone +358 20 334 443
Contact person Privacy Issues, tietosuoja@sato.fi

2. Purpose of processing of personal data

Personal data may be processed solely for the purpose of enabling SATO Corporation to fulfil its legal and ethical obligations and to ensure the appropriate investigation of reports received. The processing of personal data is based partly on mandatory legislation, such as the Act on the Protection of Persons Reporting Breaches of European Union and National Law (1171/2022) and obligations under the securities market legislation.

Processing may also be based partly on SATO Corporation's legitimate interest in investigating potential misconduct or other reported activities within its operations. Personal data is processed by individuals appointed by SATO Corporation (the whistleblowing team). Third parties and service providers may be used in connection with the processing of personal data.

3. Data file contents and regular sources of information

The data file contains information provided by SATO employees and individuals belonging to SATO's stakeholder groups. This information may include data on a person reported upon, such as their name and place of work, as well as information about reported incidents, investigation-related information, further measures relating to case management, as well as data on the completion of the case management process. Reports may also contain photographs and video recordings.

The personal data of the whistleblower may be registered if they have provided such information when submitting the report. The data provided by the reporter about themselves may also include special category personal data (such as health data). Circumstances related to the reported incident may be such that the whistleblower can be indirectly identified based on that information.

Data will be deleted from the register once it is no longer necessary for the investigation of the matter. Reports submitted pursuant to the Securities Markets Act will be retained for five years, while other reports will be deleted during the calendar year following the year in which the report was submitted. The retention period may vary due to mandatory legal requirements, for example under legislation relating to criminal proceedings and occupational health and safety.

4. Access to personal data and regular disclosures

Personal data may be accessed and processed by SATO's whistleblowing team. Data will be disclosed only to SATO's whistleblowing team and to Finnish authorities where required by law.

To ensure the proper handling and investigation of a report, the whistleblowing team may, at its discretion, involve other individuals in the handling and investigation process, such as a superior, the person responsible for the business area, and external advisers. The whistleblowing team may disclose to them such information relating to the report as it considers necessary. These individuals are also bound by confidentiality obligations.

Personal data may be disclosed to third parties, such as authorities or external auditors, where required by law.

The whistleblowing channel used by the Data Controller is maintained by an external service provider. The Data Controller has ensured through contractual arrangements that the service provider processes personal data received through the whistleblowing channel in accordance with applicable data protection legislation.

Data will not be transferred or disclosed outside the European Union or the European Economic Area.

5. Transfers of personal data outside the EU or EEA

The external service provider responsible for the technical operation of the whistleblowing channel ensures that the actual processing and storage of personal data take place within the European Union (EU) or the European Economic Area (EEA). Some of the service provider's sub-processors are based in the United States. The service provider has ensured an adequate level of data protection with these sub-processors through the following measures:

- **Contractual safeguards:** Sub-processors are required to comply strictly with legislation governing the processing of personal data (GDPR).
- **Standard Contractual Clauses (SCCs):** Where personal data may be transferred or accessed from outside the EU, the European Commission's Standard Contractual Clauses, as referred to in Article 46(2)(c) of the General Data Protection Regulation, are used. These clauses are incorporated into the agreements between the service provider and its US-based sub-processors.
- **Information security:** The service provider has ensured that the service maintains an adequate level of information security to protect the data of reporters and persons who are the subject of reports under all circumstances.

The latest versions of the Standard Contractual Clauses are available on the European Commission's website.

6. Principles of data file protection

Only SATO's whistleblowing team is authorised to access the system and process the data contained within it. Access requires the use of personal credentials. The system is protected by technical and administrative safeguards. SATO's whistleblowing team operates under strict confidentiality.

7. The data subject's rights

Personal data is not used for automated decision-making that produces legal effects concerning an individual or similarly significantly affects them.

An individual has the right, on grounds relating to their particular situation, to object to profiling concerning them and to other processing activities carried out by the Data Controller where the processing of personal data is based on the Data Controller's legitimate interests.

An objection request may be submitted in accordance with section 8 of this privacy notice. When submitting such a request, the individual must specify the particular situation on which the objection is based. The Data Controller may refuse to comply with an objection request on grounds provided by law.

An individual has the right to obtain confirmation of whether personal data concerning them is stored in the register and to access such data. Requests for access must be made in accordance with the instructions provided in this privacy notice. The right of access may be restricted on grounds provided by law. As a general rule the right of access may be exercised free of charge.

To the extent that an individual is able to do so themselves, they must, without undue delay after becoming aware of an error or upon identifying one, correct, delete or supplement any information in the register that is inaccurate, unnecessary, incomplete, outdated or otherwise inconsistent with the purpose of the register.

Where an individual is unable to correct the data themselves, a request for rectification must be submitted in accordance with section 8 of this privacy notice.

An individual also has the right to request that the Data Controller restrict the processing of their personal data, for example while awaiting the Data Controller's response to a request for rectification or erasure of their personal data.

An individual has the right to lodge a complaint with the competent supervisory authority if they believe that the Data Controller has not complied with applicable data protection legislation in its processing activities.

8. Contacts

The data subject should contact the controller in writing by email or post using a message addressed to the contact person in all matters relating to personal data processing and situations relating to the exercise of the data subject's rights.

Contacting the controller can also be done using the whistleblowing channel.

For contact details please see under section 1 'File controller'.