Stakeholder persons' Data Privacy Statement

Processing of the personal data of stakeholders in the Finnish operations of the SATO group

Date of drafting: 8 March 2021

Table of contents

1. File controller

SATO Corporation (on its own behalf and on behalf of all companies in the SATO group, hereinafter SATO)
Panuntie 4, PO Box 401
FI-00601 Helsinki, Finland
phone 020 334 443

Contact person:
Privacy issues, Panuntie 4, PO Box 401, FI-00601 Helsinki, Finland
e-mail tietosuoja@sato.fi

2. Names of data files

- purchasing and real estate data system
- stakeholder data file
- the share and shareholder register as well as bondholder register
- job application data file
- archives, photo archives and recordings
- camera surveillance
- management of the use of data systems
- data on construction and repair sites

A separate Privacy Statement has been prepared for SATO's Whistleblowing channel.

3. Purpose and legal basis of processing of personal data

SATO processes personal data on several different **legal basis**. The grounds for processing personal data are: compliance with SATO's statutory requirements, drafting and fulfilment of agreements with data subjects or companies they represent, consents of persons, and legitimate interest of SATO.

The legitimate interest of SATO may have to do with the establishment, development, termination, archiving or other upkeep of a cooperation relationship created or to be created with the data subject; review and development of SATO's business; risk assessment and management; marketing to SATO's current, former and potential stakeholders, transfer personal data between SATO Group companies, influencing in society and recruitment. The legitimate interest of SATO may also have to do with physical or information security or the need of SATO to protect its rights and assets.

For purchasing activities, personal data are collected on a contractual basis and on the basis of SATO's legitimate interest, and also on the basis of requirements under legislation (such as the Act on the Prevention of Money Laundering and Terrorist Financing 444/2017, and the Act on the Enforcement of Certain Obligations of Finland as a Member of the United Nations and of the European Union 659/1967) or based on the requirements of contractual obligations.

For material procurement purposes, personal data may be collected from the service contractor's maintenance and repair service personnel for the operation of the vendor's sales systems on a contractual basis or based on SATO's and the personnel legitimate interest. The vendor is the controller of his data system.

To the property data system can be stored the personal and contact details of the parties involved in the management of each property on the basis of the contractual relationship between the party or his/her employer and SATO.

The data required by the legislation in force in each case and the Corporate Governance Code of the Securities Market Association is collected from the persons belonging to **the company's management** and their related parties.

In addition, photographs of the members of the Board of Directors and information required for the payment of fees may be stored.

The necessary data will be collected on **rental employees** and other persons employed by SATO's contract partners working at SATO's premises on the basis of an agreement between SATO and the contractor.

Data for **stakeholder cooperation and influencing in society** are collected on the basis of valid consents and the legitimate interest of SATO.

Personal and employer data may be collected from **persons visiting** SATO's premises on the basis of SATO's legitimate interest.

A copy of his / her identification document may be kept from the person providing the **interpretation service** in order to safeguard the legitimate interests of SATO and the person in need of the interpretation service.

The share and shareholder register data and the bondholder register are maintained under the Company and Securities Markets Act.

Data on **job applicants** are collected for the purpose of carrying out the recruitment process and assessing suitability and as preparatory measures for the conclusion of an employment contract. The job application data collected for the recruitment of new employees are deemed contractually based data. Open job applications can be saved.

Direct marketing can be based on the legitimate interest of SATO, but you have the right at any time to deny that when SATO is no longer targeting you direct marketing. Electronic direct marketing is only possible if the person has given their prior consent.

Direct marketing to companies is allowed. For example, a marketing message to the address ostot@yritys.fi is allowed and the employee's work e-mail address taija.tyontekija@yritys.fi may be sent direct marketing without the person's prior consent, if the content of the marketing communication is related to the person's job duties. Even in these situations, a person has the option to prohibit direct marketing directed at him.

Data concerning marketing consent givers can be used to develop marketing communications and thereby better and personalized and more targeted communication. For this purpose, the e-mail address may be associated with the information obtained through cookies.

In order to safeguard security and legal protection, **camera surveillance** data may be collected in SATO's premises and properties and on their grounds on the basis of the legitimate interest of property owner, tenant or a third party. The data are used to investigate criminal offences and incidents of damage and real-time security control. Visible signs to indicate camera surveillance are placed in the premises and areas where cameras are located. SATO Oyj acts as the controller in case of all properties owned by companies belonging to the SATO Group. In addition, alarm and security systems may be used at SATO's premises.

Photographs can be taken at sessions and events organized by SATO. Photographs can be used in SATO's publications, but they do not include the names of the customers. Photos represent a group of people where nobody is emphasized. Only with consent of the person we can publish a photo that shows the person.

Remote meetings and other occasions can be **recorded** for business reporting, documentation of contract negotiations, orientation and other similar uses. The recording will be mentioned at the beginning of the event. The recording may include a picture of the participant, the name, the content of the discussion and the material presented at the event. Recordings can be processed when required for work tasks. SATO's right to record events may be based on a contractual relationship, a legitimate interest or the consent of the participants.

Data including user data, user names and passwords in a pseudonymized form are collected in compliance with data protection norms for **information systems** usage management and to safeguard the legitimate interest of SATO and its employees as well as contractual partners and their employees.

Personal data on **construction and repair sites** can be collected on the basis of requirements under legislation (such as the Land Use and Building Act 132/1999, the Act on the Contractor's Obligations and Liability when Work is Contracted Out 1233/2006, "Contractor's Liability Act", the Occupational Safety and Health Act 738/2002, and the Taxation Procedure Act 1558/1995), when legislation requires SATO to collect the data.

SATO has **an electronic and a paper archive** in which documents are stored to the extent required by contractual relations and legislation. At the end of the retention period, old documents may be retained in the archive for historical and filing purposes on the basis of SATO's legitimate interest.

No wholly **automated decision-making** takes place on the basis of personal data. When required by the Contractor's Liability Act, other legislation or a legitimate interest relating to SATO's business or risk management, persons may nonetheless be automatically classified on the basis of certain pre-determined criteria. Classification does not automatically result in legal or comparable impacts on the data subject, however.

Contractual or cooperation relationships can only arise on the condition that the partner or person provides the required personal data.

All personal data are kept confidential, unless otherwise required by law or otherwise stated in this Privacy Policy.

When using **strong electronic identification** services and when making electronic signatures, you must provide the identity service provider the personal information it needs, such as your identity, and act according to the instructions provided by the service provider. The service provider acts as a controller for the personal information you provide to it. You can read the current supplier's privacy statement at https://adm.signspace.com/binary/signspace_person_privacyPolicy.fi.pdf

SATO's Internet services include a real-time **chat service**.

Cookies
SATO uses cookies to the extent required by the Internet service. Cookies can be used to collect online statistics on online behavior from all users in connection with the use of SATO's Internet services. SATO does not collect personal data using cookies, unless otherwise stated in this privacy statement. Cookies are stored in the user's browser memory to enable user-specific functions, such as logging in or giving consent. In connection with the use of the Oma.sato.fi portal, the id address is stored in the cookie of the logged-in user in a pseudonymous form to identify the right of use. The cookies are mainly long-term and can remain on the user's machine for one month to four years, unless the user deletes the cookies from their machine. SATO use a third party (such as Facebook, Google, Hotjar, Giosg, Youtube, Adform, AppNexus Inc, Semasio) services, for example. monitoring the quality of internet service and targeting advertising. These service providers store their own cookies in the memory of the user's browser. Third parties do not collect the user's personal data, but use the Close enough principle to provide the service. For more information on third-party cookie functionality, visit each operator's website, for example

- www.google.com/policies/privacy/partners/
- https://fi-fi.facebook.com/policies/cookies/
- https://www.hotjar.com/legal/policies/privacy/
- https://www.giosg.com/privacy-policy
- https://www.youtube.com/intl/ALL_fi/howyoutubeworks/user-settings/privacy/
- https://site.adform.com/privacy-center/website-privacy/website-cookie-policy/
- https://www.xandr.com/privacy/
- https://www.semasio.com/privacy

The customer can block third-party cookies when arriving SATO's internet pages and cookie options are avalable. However, the customer cannot delete Giosg's cookies because they are necessary for the chat service.

4. File data content

The purchasing system may contain data on the name and contact information of the partner company's contact person, business ban, debt settlement, data required under the Contractor's Liability Act, data on the subjects of international sanctions, and data required under the Act on the Prevention of Money Laundering and Terrorist Financing. For the purchase of goods, personal information of a contractor's staff can be collected, including name, personal identification number, contact information, mobile device information, and payment card information. Personnel identification data and other information required for work are collected from rental employees and employees of the contract partner working at SATO's premises.

Data collected for **stakeholder cooperation** are a person's name, occupation, address, email address, employer and its contact information, position of person in organisation, and data relating to invitational events and mailings. The **photos** of the audience can be taken at the stakeholder events, but the

names of the people in the photos will not be recorded in the photo unless otherwise agreed with the person concerned. For marketing purposes, photographs of individuals are not used without the consent of the people present.

The data concerning the **corporate management** required by legislation and the Securities Market Association's Corporate Governance Code (https://cgfinland.fi/en/corporate-governance-code/) as well as photographs on the members of the Board of Directors and the data necessary for the payment of fees are stored. The members of the corporate management are the members of SATO Oyj's Board of Directors and the President and CEO, as well as the members of the SATO Group's Management Team.

Personal and employer information can be collected from **people visiting** SATO's premises.

A copy of his / her identification document from the person providing the **interpretation service** may be stored in connection with the information of the person in need of interpretation assistance.

The information required by law is stored as **share and shareholder register** data and **bond holder register** data, which are e.g. the name, address, sector, nationality, language, nominee register data, type of book-entry and the number and percentage of shares and bonds held.

Job application data may contain data on the applicant's name and contact details (address, phone number and email address), language skills, qualifications and studies, other education, work experience, special skills, ICT skills, references, salary request and other data reported by the job applicant and relevant to the job applied for, availability of applicant to join SATO, form and hours of employment applied for, applicant's interests and place of employment, as well as a photo, CV or free-format application. The applicant's suitability assessment, sanction compliance data, credit data and business prohibition data if any may additionally be verified and recorded in the context of job application processing, as well as other information mentioned in the law on protection of privacy in working life, if the conditions of the law are met. The data of open job applications can be stored.

We obtain information about **rental employees** or persons employed by SATO's contract partners working at SATO's premises from the person himself or from his or her employer.

Camera surveillance data contains data on the persons present in the area covered by the surveillance cameras on SATO's premises and properties and on their grounds. In addition to video footage, the data file also includes the date and time of the images recorded. No audio recording is made. The data file is made up of the transmitted digital recordings made when the cameras placed by SATO at necessary locations are in operation. Visible signs to indicate camera surveillance are placed in the premises and areas where cameras are located. SATO's premises may also have a security and alarm system.

Photo Archive. Photographs of the public may be taken at events organized by SATO, provided that the names of the persons appearing in the photographs are not recorded in connection with the photograph, unless otherwise agreed with the person concerned. Such photographs may be published in bulletins and newsletters. No personally identifiable photographs shall be used for marketing purposes without the express consent of the persons appearing in them.

Remote meetings and other occasions can be **recorded** for business reporting, documentation of contract negotiations, orientation and other similar uses. The recording will be mentioned at the beginning of the event. The recording may include a picture of the participant, the name, the content of the discussion and the material presented at the event.

Documents containing personal information may appear in the **electronic and paper archives**.

Data collected for **information system usage** management are: IP addresses, information system access rights and any restrictions therein, the access right holder's name and email address, user IDs and passwords, other identifiers such as PIN codes, and the data recorded in the context of information system usage in a pseudonymous form.

When SATO purchases **anonymisation or pseudonymisation services**, the service provider acts as the controller.

The list of parties working at own or shared **construction and repair sites** kept pursuant to the Contractor's Liability Act, the Occupational Safety and Health Act and the Taxation Procedure Act may contain:

The name of the site; the name of the principal contractor; the names of the subcontractors, the name of the client/developer, supervisor, site manager, occupational safety and health coordinator, party undertaking the construction project, contact persons, employees and independent parties performing work: the first and last name and business ID/personal identity code (or equivalent foreign identifier), facial image, nature of employment, home state, address, phone number, email address, date of birth, tax number, A1 or E101 certificate or other basis for foreign employee's right to work, employer and employer's it's business ID, with regard to posted workers the name and Finnish contact details of the representative, the worker's acknowledgement of job orientation provided, start and end dates of work at the site, and the hours and days worked and the date of returning an expired access pass as well as any business prohibitions imposed on persons belonging to company management.

Special or sensitive personal data (high-risk data) will not be stored except inadvertently in the context of camera surveillance, the recruitment process or as expressly required by law. We strive to avoid storing high-risk data. Information about a person's ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, or sexual behavior is not recorded. We may record the imposition of international sanctions, subscriber

liability information and a business ban to protect SATO's legitimate interest or as a result of a statutory obligation.

5. Regular sources of data

Purchasing and construction site systems data are collected from the service providers, the principal contractors, the employers and co-workers of persons, and persons themselves, from public data sources and from paid or free data services.

Data for the stakeholder data file are collected from public data sources, the employers and co-workers of persons, and persons themselves and from paid or free data services.

The personal data of the company's management is collected primarily from the person himself. In addition, the necessary information can be obtained from the person's family member, SATO's shareholder register, the bondholder register and the Tax Administration, as well as from other sources of information that are necessary at any given time.

Job application data are obtained from applicants and, with their consent, also the references put forward by the applicant and possibly from public data sources and from paid or free data services.

At the SATO premises, the visiting person provides his / her own information upon arrival.

Interpreters provide their own identification data.

The share and shareholder as well as bondholder register data are collected from the shareholders, bondholders or their custody banks.

The camera surveillance data file is made up of the transmitted digital recordings made when the cameras placed by SATO at necessary locations are in operation. Camera surveillance data are recorded automatically when someone enters the area under surveillance by a camera in operation.

Photographs are taken by SATO staff or a hired photographer. The recordings are made by SATO staff.

The data collected for information system usage management are obtained from the persons themselves, employers, supervisors, system administrators and SATO's IT personnel.

Credit and payment history data, data required under the Contractor's Liability Act, data collected for the prevention of money laundering and terrorist financing and sanction monitoring data may be collected and updated from sources including the data files of Suomen Asiakastieto Oy. SATO may update contact information, phone numbers and other personal data also from other reliable data sources provided by third parties for free or against a charge.

6. Data disclosures and data transfers

The file controller does not publish the data collected by it and complies with the obligation of secrecy in respect of personal data unless otherwise required by legislation or the establishment, exercise or defence of legal claims or otherwise mentioned in these records.

The share and shareholder registers as well as bond holder register data are public.

Personal data may be disclosed to authorities when they request it based on law.

Information and photographs of SATO's board and corporate management members may be published on SATO's website, in annual reports, in contact information systems or in other necessary contexts when required by SATO's interest, legislation or the Finnish Securities Market Association's Corporate Governance Code.

The photos of audience taken at SATO's events may be used as an illustration of SATO's publications within the limits permitted by law.

The data referred to in this data file description are not transferred outside the SATO group with the exception of partners, subject to a secrecy obligation and under a data protection agreement, carrying out specific tasks on behalf of the SATO group such as managing a construction or repair project, purchases of goods, maintaining the share and shareholders register as well as bondholder register, chat or interpretation services, recruitment process or security monitoring in part or information system or data security system development and maintenance, and by parties which by law are entitled to obtain the data. Data transfer is limited by purpose.The data protection agreement provides for matters including the standard of information security and reporting of information security breaches between SATO and the contractual partner, in accordance with the EU General Data Protection Regulation.

The data in the camera surveillance data file are only disclosed when a request for specific data in the file is made in writing by the police or another competent authority for a purpose specifically provided in law.

In order to maintain information systems, data may be transferred to the United States, outside the European Union or the European Economic Area only in accordance with and within EU data protection law on the basis of an EU Commission decision on the adequacy of data protection in the country of destination and for example binding rules of the group of companies accepted dy data protection authorities. More broadly, personal data is disclosed only by Euroclear Finland Oy, which maintains SATO Corporation's share and shareholder register and bondholder register. Euroclear transfers data outside the EU / EEA area using standard contractual clauses approved by the EU Commission. More information can be found at: https://www.euroclear.com/finland/en/who-we-are/gdpr.html

7. Period of storage of personal data

Other statutory data are stored for a period of six years from the end of the year in which the data were registered or, in the event of multiple registrations, in which the data were most recently registered.

Data collected on a contractual basis may be stored for a period of ten years from the end of the contractual relationship and the fulfilment of the obligations arising from it.

Stakeholder data file data are stored for as long as the relevant person holds the position due to which the data on that person were recorded unless the person has given consent for the continued processing of the data. Data removal takes place once we learn that a person no longer qualifies for the stakeholder data file, however at least every calendar year.

The data concerning Corporate Management will be stored for at least ten years from the year of publication. Information covered by accounting legislation is retained for six calendar years as part of the accounting records. Reporting data is retained for six years from the reporting year.

Photos can be stored for active use for up to 10 years after taking the photo and for archival and history purposes permanently.

Remote meetings and other occasions can be recorded for business reporting, documentation of contract negotiations, orientation and other similar uses. Recordings can be stored for up to 10 years.

Visitors' data will be retained for a maximum of one whole calendar year.

The identifier data of the interpreter is stored as part of the customer's data and the retention period is determined by the retention period of the customer's personal data.

The share and shareholder register data as well as the bondholder register data are stored at the Central Securities Depository by the law, but at least 10 years after the end of the ownership.

Job application data and open job application data are stored for a maximum of one year from the end of the application period or the receipt of an open application, unless the application results in employment

Camera surveillance data are stored for the amount of time found necessary when they contain data based on the purpose and under investigation. Data under investigation are stored for the period of time needed for the establishment, exercise or defence of legal claims. When the need for storage of the data comes to an end, the data are removed within three years. Otherwise the data are regularly destroyed by being recorded over within no more than a year of initial recording.

Documents in the electronic and paper archives may be kept for active use for a maximum of 15 years from the expiry of the document and for archival and historical purposes permanently.

Information system usage management data are stored for six calendar years from the removal of access rights.

The data collected pursuant to the Land use and Building Act, the Contractor's Liability Act, the Occupational Safety and Health Act and the Taxation Procedure Act are stored for a period of six years from the end of the year in which the site or work ended or was completed or other period required by law.

Personal data stored in SATO's acquisition and real estate register may be retained for a maximum of six years from the end of the year in which the person's position for which he or she was last entered in the register ended.

Data collected by means of cookies are stored for a maximum of five years depending on the nature of the cookie.

Data recorded on the basis of consent are removed from the data file after withdrawal of consent. If, in addition to consent, there is no other legal basis for processing the data, the data shall be deleted without undue delay. In all cases, the activity requiring consent shall cease immediately, even if the data cannot be deleted. In this case, the information about your consent and its revocation can be kept for as long as other information about you can be kept.

8. Principles of data file protection

Only designated representatives of the personnel of SATO or a contractor selected by SATO who have a legitimate need to access the data for work have the right to access the systems containing personal data and to process the data held in the systems. There is a data protection agreement between SATO and the contract partner. The use of personal identifiers is required. The system is protected through technical and administrative means.

A. Manual data / storage location and protection: Data are stored in locked and supervised premises. Only persons appointed by the SATO Group have access to the information.

B. Electronically recorded data / principles of file access and access control and physical protection of hardware: Data are only accessible by persons designated by the SATO Group. The access rights to data files are determined individually for each position. SATO's internal processes are observed in the determination of access rights. The databases and data networks used to store data are protected by means of organisational and technological measures. The supervision and protection of data files complies with regulations applied within the EU.

9. Right of access to own personal data

Persons have right to receive from the file controller confirmation as to whether personal data concerning them is being processed.

Persons have the right to access their own personal data. The right of access may only be refused pursuant to legislation. The request for right of access may be made to the controller in writing. Please submit any written requests for right to access to the data protection contact person at SATO Corporation at

the address PO Box 401, FI-00601 Helsinki, Finland or by email to tietosuoja@sato.fi.

Photos, camera surveillance data, cookie information and system usage log data cannot be disclosed because these materials would contain the personal data of other people or the compilation of the materials would be unduly burdensome.

The right of access is provided without delay and no later than within one months of the submission of the request. In exceptional situations, the delivery time may not exceed three months.

The data will be supplied to the person concerned in single copy in person against verification of identity, or by other protected means using reliable identification. Requests submitted electronically will be complied with electronically when possible in terms of information security.

If the request for access is manifestly without foundation or unreasonable, and especially when the requests are made repeatedly or if more than one copy is requested, the controller may charge for compliance with the request a reasonable fee, based on administrative costs, or refuse to comply with the request.

The holder of a share or bond may check the details of his or her holdings using the Euroclear CSD Customer Interface.

10. Rectification or removal of personal data and right to request restriction of processing

Persons may request the rectification of erroneous data, in which case the decision regarding data rectification is made by the controller. The controller may rectify incorrect data detected after receiving the correct data from the person concerned or another reliable source.

Insofar as the person is capable of taking personal action, they must, without undue delay after having been informed of or having personally detected an error, on their own initiative rectify, erase or supplement personal data contained in the data file that is contrary to the purpose of the file, incorrect, unnecessary, incomplete or obsolete. Persons are responsible for keeping any personal user ID and password confidential and for any usage taking place with the personal user ID.

Persons have the right to have the personal data concerning them erased from the data file ('right to be forgotten') after the end of the storage period if their personal data are no longer needed for the purposes for which they were collected, the person objects to processing for which there are no legitimate grounds, consent is withdrawn in respect of processing based on consent, or the personal data have been unlawfully processed or the controller is obligated under law to erase the data or the period of storage has expired. The controller will decide, in compliance with legislation in force from time to time, on the erasure of data without undue delay.

Persons also have the right to ask the controller to restrict the processing of their personal data when

- a request for rectification or removal of their personal data is pending with the controller;
- the processing is unlawful but the person does not wish the data to be erased but instead asks that the processing of the data be restricted;
- the controller no longer needs the said personal data for processing purposes but the data subject needs the data for the establishment, exercise or defence of a legal claim;
- the person has objected to the processing of the personal data pending the verification whether the legitimate grounds of the controller override those of the person (the balance test).

When processing is restricted on the aforementioned grounds, such personal data may, with the exception of storage, only be processed with the person's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

11. Right to object to processing on grounds relating to particular situation

Persons have the right, on grounds relating to their particular situation, at any time to object to the controller processing their personal data pursuant to the controller's legitimate interest.

The objection specifying the grounds on which the person objects to the processing may be submitted to the contact person of the file controller in this data file description. The controller may refuse to implement a request concerning an objection on grounds laid down in legislation after completing the necessary balance test between your and SATO's legitimate interests.

12. Right to prohibit direct marketing

Where personal data are processed for direct marketing purposes, persons may at any time object to the processing of their personal data for such marketing, which includes profiling to the extent that it is related to such direct marketing. If a person objects to the processing of his or her personal data for direct marketing, the data may no longer be processed for that purpose.

13. Right to withdraw consent

Persons has the right to withdraw their consent to the processing of their personal data at any time, insofar as processing of personal data is based on his / her own consent. The withdrawal of consent does not affect the lawfulness of processing based on consent before the withdrawal. A person also has the right at any time to prohibit the use of electronic channels in direct marketing targeted to her or him.

14. Right to data portability

Persons have the right to have their personal data, which they have provided to the controller and which are processed by the controller on the basis of

consent or contractual relationship, transmitted in machine-readable format to another controller when this is technically feasible and secure.

If the transfer is not technically feasible or secure, persons may supply another controller with their personal data which they have received on the basis of the right of access.

15. Right to complain to a supervisory authority

Persons have the right to file a complaint with the competent supervisory authority in the EU Member State where he or she has a permanent place of residence or workplace or where the alleged breach of the Data Protection Regulation has occurred. The competent authority in Finland is the Data Protection Ombudsman (Ratapihantie 9, PO Box 800, 00521 Helsinki or email: tietosuoja@om.fi). For more information, please visit the Data Protection Ombudsman page tietosuoja.fi.

16. Contacts

In all matters relating to the processing of personal data and in situations involving the exercise of your rights, you may contact the controller in writing, either by e-mail or by post, to the controller's contact person.

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