

SSAB privacy statement for whistleblowing channels

Last updated February 2023

This Privacy Statement informs about the processing of personal data by SSAB group companies including SSAB AB and its affiliates Tibnor and Ruukki, among others ("SSAB"), in its whistleblowing channels. It answers the questions of what personal data SSAB collects, uses or shares, for what purposes the data is collected and what rights persons have in relation to the processing of personal data in connection with the whistleblowing channels.

SSAB strives to achieve an open corporate climate and high business ethics. The whistleblowing systems provide a confidential way for employees and external stakeholders to report suspected violations of laws or regulations, SSAB's Code of Conduct or company policies.

This Privacy Statement describes how SSAB processes personal data in the following reporting channels:

1) Internal reporting channels

SSAB has introduced internal reporting channels that are available in certain companies belonging to SSAB Group, as required by EU whistleblower directive (2019/1937) and national laws implementing the said directive (hereafter referred to as "Internal Reporting Channels"). The reports on violations submitted through the Internal Reporting Channels are handled by specially appointed persons in each company. In summary, the internal reporting channels can be used by employees, job applicants, volunteers, consultants and certain other stakeholders, for example, if the matter concerns reporting in a work-related context of misconduct where there is a public interest in it emerging or it violates EU law (e.g. environmental protection, protection of personal data, product safety).

2) Ethics Line process

In addition to Internal Reporting Channels, SSAB has made available a centralized reporting channel, Ethics Line, where employees and external stakeholders can report suspected violations of laws or regulations, SSAB's Code of Conduct or company policies.

1. DATA CONTROLLERS

The data controller responsible for the personal data processing activities in Ethics Line is SSAB AB (registration number: 556016-3429, address: P.O. Box 70, SE-101 21 Stockholm, Sweden). This includes accountability for all data processing on a corporate level. SSAB is responsible for ensuring that personal data is processed in compliance with this Statement and applicable data protection laws.

In addition, SSAB affiliate can also be regarded as the data controller when the processing of personal data in Ethics Line reports takes place in connection to a separate contractual relationship, such as employment relationship between the employee and the legal entity acting as the employer

company, or in connection with certain statutory personal data processing and compliance with local legal requirements of an individual legal entity part of the SSAB group.

The local SSAB affiliate is also the data controller with respect to data received through its own Internal Reporting Channel.

SSAB group companies also share personal data for administrative purposes and to facilitate the business operations of the group and the individual legal entities, unless such sharing would be against the applicable legislation or the EU whistleblower directive. The information of SSAB group companies and affiliates can be found in the latest Annual Report at <https://www.ssab.com/en/company/investors/reports-and-presentations> and at <https://www.ssab.com/en/company/about-ssab/our-business>. Regardless of the data controller in a specific situation, the primary contact for privacy matters in SSAB is: email: data.privacy@ssab.com.

2. LEGAL BASIS AND PURPOSE OF PROCESSING PERSONAL DATA

2.1 Ethics Line

SSAB processes personal data within Ethics Line for the purpose of administering and investigating reported irregularities and for taking measures in connection with established violations.

SSAB processes personal data in Ethics Line with the support of a so-called balancing of interests. SSAB has a legitimate interest in enabling employees and external persons to report misconduct in Ethics Line and has assessed that this interest outweighs the data subjects' interest in privacy protection. SSAB may process personal data on violations of the law, SSAB's Code of Conduct or company policies that include suspected or confirmed crimes. Such processing may take place in accordance with local law or when such processing is necessary to establish, assert or defend a legal claim.

In some cases, SSAB may also process personal data in order to take legal action in connection with a reported matter. The legal basis for the processing is SSAB's legitimate interest in being able to take action in connection with the reported matter and has judged that this interest outweighs the data subjects' interest in protection of privacy.

To the extent that SSAB needs to process sensitive personal data or data on breaches of the law, this processing takes place on the basis that it is necessary to establish, assert or defend a legal claim. The legal basis for the processing of sensitive personal data may also be that the processing is necessary for a public important interest, on the basis of Union law or the national law of the EU member states. In some cases, SSAB may also process sensitive personal data when it is necessary to fulfil obligations and exercise special rights in the area of labor law and in the areas of social security and social protection.

2.4 Internal Reporting Channels

According to EU Directive 2019/1937 on the protection of persons who report breaches of Union law and according to the national law in the EU member states by which the directive has been

implemented, SSAB is obliged to establish internal reporting channels for whistleblowing. SSAB processes personal data for the purpose of handling and investigating whistleblowing cases that it has received via Internal Reporting Channels.

Personal data processed in the Internal Reporting Channels may also be processed for fulfilling a disclosure which:

- 1) is necessary to take action in connection with what has emerged in a reported case;
- 2) is necessary for reports to be used as evidence in legal proceedings; and
- 3) takes place in accordance with applicable law and regulation.

The legal basis for processing personal data in connection with cases received via Internal Reporting Channels is to fulfil SSAB's legal obligation of making Internal Reporting Channels available for reporting.

Depending on the nature of the whistleblowing case, SSAB may process sensitive personal data. The legal basis for the processing of sensitive personal data is that the processing is necessary for a public important interest, on the basis of Union law or the national law of the EU member states. In some cases, SSAB may also process sensitive personal data when it is necessary to fulfil obligations and exercise special rights in the area of labor law and in the areas of social security and social protection.

SSAB may also process personal data on offenses that include suspected or confirmed crimes. Such processing is necessary to fulfil SSAB's legal obligation of making available Internal Reporting Channels.

In some cases, SSAB may also process personal data in order to take legal action in connection with a report in which case such processing is based on SSAB's legitimate interest to take such measures. To the extent that SSAB needs to process sensitive personal data or data on breaches of the law, this is done on the basis that it is necessary to establish, assert or defend a legal claim.

3. COLLECTION OF DATA

Reports in the Ethics Line and the Internal Reporting Channels may contain different types of personal data. The information may be attributable to the person who submitted the notification, the person to whom the notification relates to or any other person mentioned in the notification.

Personal data that may be processed in connection with a report are:

- Basic personal data (name, address, city, gender and nationality)
- Contact information (including telephone number)
- Roles and functions
- Details of the reported event
- Actions taken
- Investigation reports
- Other types of personal data collected during the investigation, e.g. during potential interviews but also via telephone logs, data files, audio files, IP address and other technical data as well as e-mail.

Please be aware that the information you supply about yourself, your colleagues, other persons or any aspect of the company's operations may result in decisions that affect others. Therefore, we ask that you only provide information that, to the best of your knowledge, is correct and factual.

Ethics Line and Internal Reporting Channels are not intended to obtain sensitive personal information, such as data that can disclose a person's racial origin or ethnicity, religious or other beliefs, political opinions, membership of parties, trade unions, health, or sex life. If this type of information will be provided, the information will only be processed if there is a legal basis to do so, as described in section 2 of this statement.

The whistleblowing reports are treated in confidence, and the person processing a report must not disclose any information that could reveal the identity of the whistleblower or any other individual involved in the case to unauthorized parties. The information you submit will be treated confidentially except in cases where this is not possible because of legal requirements or in order to conduct a proper investigation, in which case the information will be handled sensitively. We encourage you to identify yourself in order for us to follow up with questions we may have.

4. SHARING OF DATA

For the purpose of processing and investigating your report and subject to the provisions of local law, the personal data and information you provide may be accessed, processed and used by the relevant personnel of SSAB.

SSAB may also disclose and outsource the processing of personal data to trusted services providers who operate Ethics Line and the Internal Reporting Channels, audit firms, legal service providers and forensic investigators, or other service providers that are necessary to detect, investigate and remedy serious violations, or for the establishment, exercise or defense of legal claims, to the extent allowed by applicable legislation and EU whistleblower directive.

The Ethics Line system is provided by People Intouch B.V who processes data only on behalf of SSAB.

When a third party acts as a personal data processor to SSAB, the supplier has, through a data processing agreement, undertaken to e.g. only process personal data in accordance with SSAB's instructions and to impose the same obligations on all its subcontractors through written agreements.

Personal data and information may also be disclosed to the police and/or other enforcement or regulatory authorities if considered necessary.

5. TRANSFER OF PERSONAL DATA OUTSIDE OF THE EU/EEA

5.1 Intra-group transfers

As some of SSAB group companies are located outside of the EU/EEA, personal data may be transferred outside of EU/EEA. This may be necessary for example due to circumstances of the reported case, for example in case the reported incident relates to activities of SSAB companies located outside EEA. In this case, these persons are required to access employees' personal data because of their work-related duties, and access to personal data is managed with limited access rights.

SSAB provides appropriate safeguard mechanisms for international data transfers as required by applicable data protection laws. For intra-group transfers, SSAB will ensure the appropriate safeguards for the protection of personal data, including by using the Standard Contractual Clauses approved by the European Commission.

5.2 Trusted service providers located outside of EU/EEA

Some SSAB's trusted service providers may process personal data outside of EU/EEA. To the extent personal data is transferred to a country outside of the EU/EEA, SSAB will use the required established mechanisms that allow the transfer to service providers in those third countries, including the Standard Contractual Clauses approved by the European Commission.

All personal data reports in Ethics Line are stored in the EU.

Please contact data.privacy@ssab.com in further questions related to international data transfers.

6. RETENTION OF PERSONAL DATA

The personal data will only be stored for as long as is necessary to investigate a report and to take relevant measures in relation to the results of such an investigation. Personal data that appears in a follow-up case is never processed for more than two years after the case was closed, unless otherwise provided in the nationally applicable legislation.

Excess personal data and personal data that are not relevant to the reported event will be deleted as soon as possible.

Personal data processed to establish, assert or defend a legal claim will be stored until the legal proceedings are completed and during the subsequent limitation period.

Written reports and documentation of oral reporting for the Internal Reporting Channels shall be kept for as long as necessary, but not longer than two years after a follow-up case has been closed unless otherwise provided in the nationally applicable legislation.

7. PRIVACY RIGHTS

You have the right to request access to personal data that SSAB holds about you. However, there may be some restrictions in this respect. Please note that what comes to personal data reported through whistleblowing channels, SSAB will not be able to fulfil the request for access if the disclosure of data may jeopardize the investigation. SSAB will promptly notify any person who is the subject of a report except where notice needs to be delayed to ensure the integrity of the investigation and preservation of relevant information.

You also have the right, to the extent required by applicable local law, to

- request rectification of personal information in case the information is incorrect;
- under certain circumstances, request erasure and/or restriction of the processing of personal information;
- object to the processing of personal information if processing is based on legitimate interest;
- lodge a complaint to the supervisory authority regarding how SSAB processes your personal information.

However, please note that certain information is strictly necessary in order to fulfil the purposes defined in this Statement and may also be required by law. Therefore, the deletion of such data may not be allowed by applicable law which prescribes mandatory retention periods or if there is an overriding interest to keep processing the data for the intended purpose.

Please send above-mentioned requests to SSAB at data.privacy@ssab.com. Any requests related to the exercise of privacy rights will be responded within one month or within the applicable regulatory time limit.

8. CHANGES TO THIS PRIVACY STATEMENT

SSAB may amend this Privacy Statement and the related information. SSAB will always provide the date of the Privacy Statement to allow the Users to see changes. Please note that this Privacy Statement is for information purposes only. SSAB will inform Users of any substantial changes by using reasonable and available channels.

9. CONTACT SSAB

For requests regarding SSAB's Privacy Statement or personal data SSAB holds about the User in question, please contact SSAB by email at data.privacy@ssab.com.