General Privacy information

Last updated: January 2025

SSAB is bound by the privacy legislation within each jurisdiction in which it operates. Sometimes the privacy legislation and the data subject's rights in relation to privacy differs from one jurisdiction to another. In addition, specific privacy practices may be adopted to address the specific privacy requirements of particular jurisdictions. Therefore, if the privacy notices are in conflict with the law of the jurisdiction in question, the local law takes precedence to the extent applicable.

SSAB has nominated a Group Data Protection Officer (DPO), who can be contacted for additional information or any inquiries or requests on personal data processing by SSAB. More information can be found in section nr. 2.

1. Data Controller

The data controller responsible for the SSAB group's personal data processing activities 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 these notices and applicable data protection laws.

In addition, other SSAB group companies can be regarded as the data controller in separate contractual or other cooperation relationship 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. SSAB group companies also share personal data for administrative purposes and to facilitate the business operations of the group and the individual legal entities. The information of SSAB group companies and affiliates can be found in the latest Annual Report. Regardless of the data controller in a specific situation, the primary contact for privacy matters at SSAB is the SSAB Group Data Protection Officer.

2. Data Protection Officer's (DPO) contact details

SSAB's global Data Privacy Organization supports with any data protection and data privacy related requests or any other questions, concerns, comments or complaints.
SSAB has also nominated a Group Data Protection Officer (DPO) who performs the following tasks:

- Informs and advises SSAB organization and its employees about obligations pursuant to the EU General Data Protection Regulation (GDPR) and to other Union or Member State data protection provisions in relation to the data processing carried out by SSAB,
- Monitors compliance with the GDPR and with other Union or Member State data protection provisions and with SSAB's policies related to the protection of personal data,

- Takes care of assignment of responsibilities, data protection awareness and training of employees involved in processing operations, and the related audits, and
- Provides advice on data protection impact assessments and monitoring their performance.

The DPO also co-operates with the supervisory authority and acts as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, regarding any other matter.

SSAB's Data Privacy Organization and the Group Data Protection Officer (DPO) can be contacted at data . privacy (at) ssab . com.

3. Transfer or disclosure of personal data

SSAB may transfer or disclose individuals' personal data to the following third parties:

- other SSAB group companies for internal processing;
- when permitted or required by law to comply with requests by competent public authorities such as subpoenas or similarly binding acts;
- trusted service providers or SSAB partners, such as suppliers, agents, distributors and marketing service providers.
- if SSAB is involved in a merger, acquisition, or sale of all or a portion of its assets; and
- when SSAB believes in good faith that disclosure is necessary to protect SSAB's rights, protect individuals' safety or the safety of others, investigate fraud, or respond to a government request.

Third parties may act as independent data controllers, or data processors, depending on the case.

4. Transfer of personal data outside of the EU/EEA

4.1 Intra - group transfers

As some SSAB group companies are located outside of the EU/EEA, individuals' personal data may be transferred outside of EU/EEA. In these circumstances, SSAB will use the required established mechanisms for the transfer outside of the EU/EEA, such as the Standard Contractual Clauses approved by the European Commission.

4.2 Service providers and other data recipients located outside of the EU/EEA

SSAB may use service providers for the personal data processing and personal data may be transferred to countries outside of the EU/EEA. SSAB will use the required established mechanisms that allow the transfer of personal data to third countries, such as the Standard Contractual Clauses approved by the European Commission and additional safeguards.

5. Security

SSAB maintains adequate physical, technical and organizational security measures to protect personal data from loss, destruction, misuse, and unauthorized access or disclosure. For example, SSAB limits access to this information to authorized employees and contractors who need to know that information in the course of their work or assignment and to third party service providers who may only process data in accordance with instructions provided by SSAB.

Please be aware that although SSAB endeavors to provide adequate security measures for personal data, no security system can prevent all potential security breaches.

6. Your privacy rights

Based on the applicable data protection laws, you may be entitled to exercise privacy rights in relation to your personal data to which SSAB acts as a data controller. You may have, subject to applicable laws, the right to:

- receive confirmation on whether your personal data is being processed, and if so, obtain access to that personal data;
- request correction of any inaccuracies regarding your personal data;
- request deletion of your personal data;
- request restriction of processing of your personal data;
- data portability of your actively provided personal data;
- object processing of your personal data based on reasons specific to your situation;
- withdraw your previously given consent for processing your personal data.

Please note that in certain circumstances, local laws and legislations may limit the exercise of specific privacy rights. For exercising your rights, please contact the SSAB's Data Privacy Organization at data.privacy@ssab.com. In addition, you always have the right to approach, make a request or file a complaint to the competent data protection authority.

7. Changes to privacy notices

From time to time, SSAB may amend privacy notices and SSAB recommends you to regularly access them to find about the latest version. Please note that these privacy notices are for information purposes only. When required, SSAB will inform individuals of any substantial changes by using reasonable and available channels.

Whistleblowing

1. Legal basis and purpose of processing personal data

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.

1.1 SSAB's Ethics Line

SSAB has made available a centralized Group-wide 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.

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.

PROCESSING ACTIVITY	LEGAL BASIS	DESCRIPTION
Reporting of misconduct	Legitimate interest | Legal obligation	Enabling employees and external persons to report misconduct in Ethics Line. SSAB 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 misconduct or 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.
Legal actions	Legitimate interest	In some cases, SSAB may also process personal data in order to take legal action in connection with a reported matter. SSAB has to be 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.
Investigating on breaches of the law	Public interest | Legal obligation	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. 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.

1.2 SSAB's Internal Reporting Channels for whistleblowing

According to EU Directive 2019/1937 on the protection of persons who report breaches of Union law (the "EU whistleblower directive") 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 ("Internal Reporting Channels"). 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.

PROCESSING ACTIVITY	LEGAL BASIS	DESCRIPTION
Investigating cases via Internal Reporting channels	Legal obligation	Processing personal data in connection with cases received via Internal Reporting Channels, which SSAB is required to make available for reporting.
Whistleblowing	Public interest | Legal obligation	Depending on the nature of the whistleblowing case, SSAB may process sensitive personal data. 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.
Investigating offenses	Legal obligation	SSAB may also process personal data on offenses that include suspected or confirmed crimes. Such processing is necessary as it is required to make Internal Reporting Channels available.
Legal actions	Legitimate interest	In some cases, SSAB may also process personal data in order to take legal action in connection with a report. 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.

Personal data processed in a follow-up case received via the Internal Reporting Channels may only be processed by persons who, on behalf of SSAB, have been designated to be authorized to receive, follow up and provide feedback on reports. Access to personal data shall be limited to what each of the authorized persons needs in order to be able to perform their tasks. The person handling a follow-up case may not disclose information that may reveal the identity of the

reporting person or anyone else who appears in the case without having authorization for the disclosure.

2. Collection of personal 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.

Reports can be submitted as anonymous, but it is possible that some personal data may be processed in connection with a report. Reports may contain personal data, such as:

PERSONAL DATA	**EXAMPLES**
Detailed personal data of reporter or reported individual (if disclosed)	Name, gender and nationality
Contact information (if disclosed)	Email address, telephone number address, city
Roles and functions of reporter or reported individual	Job title, internal duties
Details of the reported event	Content of the reported event
Actions taken	Mitigation measures and actions taken to resolve the event
Investigation reports	Investigation reports of the event
Other personal data collected during the investigation	Information collected during interviews but also via telephone logs, data files, audio files, IP address and other technical data as well as email.
Case specific data	In some cases, depending on the nature of the case, sensitive personal data may also be processed, such as racial or ethnic origin data, political opinions, religious or philosophical beliefs, union membership, information about health or sex life.

Ethics Line and Internal Reporting Channels are not intended to obtain sensitive personal data. 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 above.

A report may also mean that SSAB will process personal data on violations of the law that include suspected or confirmed crimes.

As a rule, this personal data is collected directly from employees. However, personal data related to reports concerning the Ethics Line and Internal Reporting Channels may also be collected from other sources, such as from the immediate superior, other employees, witnesses and external stakeholders.

Reports in the Ethics Line and the Internal Reporting Channels 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 individua 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.

3. Transfers or disclosure of personal data

SSAB may transfer, disclose and outsource the processing of personal data to third parties, if necessary to fulfil the purposes of the processing of personal data within the Ethics Line and the Internal Reporting Channels. Third parties can e.g., be service providers that operate Ethics Line and the Internal Reporting Channels, audit firms, legal service providers, 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.

SSAB may also share personal data with the police and / or other relevant authorities, supervisory bodies or courts in order to safeguard SSAB's interests or exercise SSAB's rights.

The Ethics Line system is provided by People Intouch B.V. All personal data reports in Ethics Line are stored in the EU.

4. 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.

5. Exceptions to privacy rights

Individuals have the right to exercise their privacy rights as mentioned in the General Privacy Info. However, there may be some restrictions in this respect.

- Please note that certain information is strictly necessary in order to fulfil the purposes defined in this notice 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 note that what comes to personal data reported through Ethics Line or Internal Reporting Channels, SSAB will not fulfill the employee's request for access if the disclosure of an employee's personal data may jeopardize the investigation.
- If SSAB receives a report via Ethics Line or the Internal Reporting Channels that contain personal data, or if personal data is collected during an investigation, SSAB will, if possible, inform the persons concerned. However, if the provision of such information may jeopardize the investigation, such information shall be provided only when such a risk no longer exists.