BOLIDEN

Data Privacy Policy

1 OBJECTIVES

All processing of personal data by Boliden must be carried out in a manner that ensures that the processing is lawful and complies with the basic principles for processing in the applicable data protection law and that enables the individual whose information is being processed (employees, customers, suppliers, etc.) to feel confident about our data handling. It is the responsibility of each employee to comply with this policy in any and all processing of personal data which that employee carries out as part of his/her day-to-day work.

2 DEFINITIONS AND EXPLANATIONS

The following definitions are used in this policy:

Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, with the help of an 'identifier', i.e. a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Processing

Any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller

A natural or legal person, such as Boliden, which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3 SCOPE AND RESPONSIBILITIES

This policy for processing of personal data applies for all companies and employees within Boliden.

It is the responsibility of each employee to comply with this policy in any and all processing of personal data which that employee carries out as part of his/her day-to-day work.

The overall responsibility for Boliden's compliance with this policy rests with the following:

3.1 CEO

The CEO must ensure that there is a suitable organisation, delegated responsibility and tasks, and sufficient resources for the work involved in processing of personal data within the company.

3.2 Data privacy organisation

Boliden has established a data privacy organisation that is tasked with providing Boliden's organisation with support on how to comply with the applicable data protection law. This task includes implementing and verifying Boliden's GDPR compliance, providing guidance and recommendations on the balancing of risk, and in relevant forums (Data Privacy Council and, when applicable, in HR/Legal Board) making data protection-related decisions.

The data privacy organisation comprises the following roles and forums:

3.2.1 Data Privacy Council

The Data Privacy Council should be represented by the following roles/departments with at least one representative from Group Management:

- Corporate Responsibility
- Legal
- HR
- Mines
- Smelters
- Data Protection Officer (DPO)

The Data Privacy Council shall:

- decide upon strategies, priorities, resources and budget; and
- based on the above, instruct and have a dialogue with the DPO.

3.2.1 HR/Legal Board

The HR/Legal board is represented by: Group Management and representatives from HR and/ or Legal depending on issue to be discussed. The HR/Legal Board shall:

- ensure data privacy is a standing item on the agenda; and
- receive information and legal advice from DPO.

3.2.2 Data Privacy Supervisors

The Data Privacy Supervisors consists of the Data Protection Officer (“DPO”) and the Data Privacy Coordinator.

3.2.2.1 DPO

Boliden has appointed a Data Protection Officer (DPO) in order to inform and advise, be an escalation point for data protection issues, and to monitor compliance as regards Boliden’s processing of personal data. The DPO must also cooperate with and be the contact point for the supervisory authorities. The DPO shall have a comprehensive view of Boliden’s compliance and the greatest risks, as well as the work on these. The DPO will report to the Data Privacy Council and HR/Legal Board and, if needed, directly to Boliden’s management team.

3.2.2.2 Data Privacy Coordinator

The Data Privacy Coordinator is responsible for the overall coordination of Boliden’s GDPR work, with focus on supporting the data privacy organisation,. The Data Privacy coordinator reports to Director of HR Group.

The Data Privacy Coordinator has a co-ordinating anchor role within the data privacy organisation (“spindeln i nätet”), and shall:

- co-ordinate and drive the data privacy organisation and
- co-ordinate and drive data privacy matters (based on advice from the DPO).

3.2.3 Process and Information owners

3.2.3.1 Business Area/Group Functions

Delegates changes to regulation, adjacent laws or other updates/clarifications and requirements.

3.2.3.2 General Managers/Business Unit and Director Group Functions

The GM and Dir Group functions have the responsibility but can delegate work to Data Privacy Champions, and shall:

- provide support, guidance and suggestions to balance risk;
- put in place appropriate technical and organizational measures (e.g. steering documents, templates, data protection by default and by design);
- specific legal advice; and
- specific advice on IT matters

3.2.3.3 Data Privacy Champions

A Data Privacy Champion is an appointed person designated to be a locally responsible at site/business area/group function. The appointed person is

often a local HR person, but it is possible to appoint additional persons as Data Privacy Champions at a site/business area/group function for example, a local IT, or local camera surveillance responsible.

Data Privacy Champions are the primary contacts for all employees in data privacy matters and shall reach the entire organisation and ensure that actions are implemented. Data Privacy Champions are responsible for implementing the priority actions in the organisation, such as:

- implementing steering documents;
- implement data processing agreements;
- educate and inform employees (supported by Data privacy Supervisors);
- implement new/changed routines and processes;
- specify requirements for changes to IT systems;

Data Privacy Champions shall also:

- work together with Data Privacy Supervisors to develop plans and specify estimates for the implementation of actions;
- report to Data Privacy Supervisors;
- flag to Data Privacy Supervisors when detecting new processes or collecting of new personal data to determine legitimate basis, updating information to data subject etc.;
- users of the processing records responsible for ensuring that the processing record is updated (new or changed processing's);
- flag on suspicion of personal data breach to DPO or Data Privacy Supervisors;

- if necessary, participate in the work of carrying out requests from data subjects.

3.2.3.4 System Support (Application manager)

Application manager shall:

- take responsibility for ensuring GDPR compliance;
- establishing and supervising GDPR compliance (Privacy by design and privacy by default); and
- implement appropriated security measures in line with Boliden Data privacy Policy

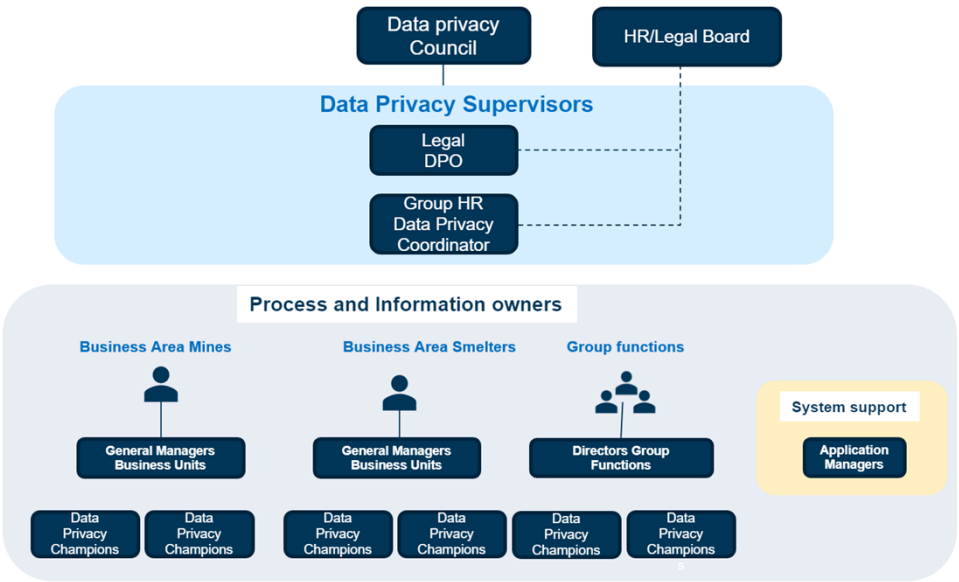


Figure 1: Data privacy organisation, schematic view

3.2.4 Employees

Each employee is responsible in his/her day-to-day work for lawful and fair processing of personal data. By following the Boliden Group's steering documents in respect of processing of personal data, the employee is contributing to the satisfactory processing of personal data.

4 POLICY

Boliden must implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the applicable data protection law.

Boliden must, in the processing of personal data, comply with the principles set out in the General Data Protection Regulation (GDPR), meaning that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Boliden must be able to demonstrate compliance with these principles, and Boliden's processing of personal data must for that purpose be documented in a structured and clear manner.

Boliden must take appropriate measures to respect the rights of data subjects.

Boliden must ensure that any new system or processing procedure that is introduced within the Group and which includes processing of personal data is designed in such a way that effective protection of the personal data is integrated into the processing (data protection by design).

Boliden must further ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility (data protection by default).

Boliden must ensure a level of security of processing that is appropriate to the risk.

Boliden must cooperate with the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten) (or other relevant supervisory authority) in the performance of its tasks.

In the drawing up of contracts, Boliden must, if applicable, ensure that there is a written data processing agreement that regulates the processor's processing of personal data.

5 PERSONAL DATA TRANSFERS OUTSIDE THE EU AND EEA

Boliden must ensure that any transfer of personal data outside of the EU/EEA, to so called third countries, is subject to appropriate safeguards and that the level of protection of the data transferred is essential equivalent to the EU standard. In its judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) states that controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools.

To ensure the effectiveness of the transfer tool (which for Boliden most often will be the so called, standard contractual clauses) a Transfer Impact Assessment (TIA) shall be done before the start of a processing activity that includes a transfer. The TIA shall be done in parallel with the planning, procurement and/or development process and shall include the steps outlined in Boliden's Data Transfer Impact Assessment Template.

BOLIDEN

6 6. BREACHES

Breaches of this policy must be reported to the DPO (Data Protection Officer) by phone or e-mail (dpo@boliden.com). It is important that the breach is reported as soon as possible.

7 DETAILED INFORMATION

For further information, see guidelines, instructions and tools in the Data Privacy Portal on Boliden ´s Intranet.

8 POLICY AUDIT CHECK LIST

Compliance with this policy may be subject to an internal audit. In order to ensure compliance with the policy within your organisation, the following questions must be answered with 'Yes'.

1) Is there a Data Privacy Champion appointed at your site/business area/group function?
2) Is personal data processed according to the principles set out in this policy?
3) Are there processes and routines for processing of sensitive personal data?
4) Are these processes documented?
5) Is there a visible audit trail?
6) Are the processes and routines in line with this policy?
7) Are all employees aware of this policy, the guidelines and the processes and routines?
8) Are breaches of this policy reported to your local Data Privacy Champion?