Information about processing of personal data Whistleblowing function

Below is information about the processing of personal data that takes place in connection with our handling of whistleblowing cases and your rights as registered.

Controller

The party responsible for the processing of personal data, the controller, is:
Svedbergs i Dalstorp AB, 556052-4984
Verkstadsvägen 1
514 63 Dalstorp, Sverige
Telephone: 0321 53 30 00
E-mail: gdpr@svedbergs.se

For additional information regarding our processing of personal data, see the from time-to-time applicable Svedberg's Privacy Policy.

Purpose of processing and legal basis

The purpose with the processing is to fulfil the legal requirement put on the organization to have a whistleblowing function and to be able to investigate the incoming whistleblowing cases. The purpose is also to process personal data when it is necessary to follow up whistleblowing cases. This means we might need to process personal data to be able to:

- Manage reported whistleblowing cases,
- Protect the organisations' rights and obligations in light of the reported irregularities.
- Fulfil the legal requirements put on the organisation.

The legal basis for the processing of personal data in whistleblowing cases is the legal obligation in 5 chapter 2 § in the Swedish whistleblowing law (2021:890).

The legal basis for the processing of personal data when following up whistleblowing cases and when taking other measures in relation to a whistleblowing case is to comply with a legal obligation or the organisation's legitimate interest in looking after its rights in relation to reported irregularities.

Categories of data subjects

Personal data of the following categories of data subjects can be processed when handling whistleblowing cases:

- The reporting data subject, if she or he doesn't choose to be anonymous,
- Data subjects mentioned in a whistleblowing case,
- Data subjects with the administrative role to manage and investigate whistleblowing cases.

Data transfer

Data may be provided to public authorities (e.g., the Swedish police authority when a whistleblowing case leads to a police report) in compliance with legislation. Data may also be provided to other parts of our organization or another company within our group when investigating and following up whistleblowing cases.

Personal data is also processed by processors when we handle whistleblowing cases. Processors are only allowed to act on instructions from us which is regulated in a data processing agreement.

Transfer to a third country

We strive not to transfer data to a country or company located outside the EU/EEA and all personal data related to the content in reported whistleblowing cases is stored within the EU/EEA on servers owned by Swedish companies.

Log in and access to the whistleblowing system is administrated through active directory, Microsoft Azure. The data is stored within the EU/EEA but the supplier of the service is an American company, this means personal data related to log in and access administration might be accessed by American authorities which could have a negative effect on the data subjects privacy since American authorities aren't bound by the GDPR. If personal data is transferred to a third country, standard contractual clauses are in place as appropriate safeguards. Please contact us for more information on how we protect your personal data.

Retention and deletion

The personal data included in a whistleblowing case will be kept for two years from when the case was closed.
The personal data which is needed for administration and to manage log in and access to the whistleblowing system will be kept for as long as the log in and access is valid.
All personal data will be deleted when the retention period ends.
If a whistleblowing case needs further internal investigation, the personal data will be kept for as long as it is needed to investigate the case.

Your rights as a data subject

When the company collects and processes your personal data, you have certain rights. You have the right to:

- Request a copy of the personal data that the company processes and details of how the data are processed.
- Request the rectification of any inaccurate data.
- Request to be erased. However, this can only be done provided that there is no other legal basis giving the company the right to retain the data.
- Request that processing be restricted under certain circumstances, such as during a period when the correctness of the data is under investigation.
- Exercise the right to data portability.
- Oppose to profiling.
- Lodge a complaint with the data protection authority (in Sweden Swedish Authority for privacy protection IMY) regarding our processing of personal data.

Please note that the rights above can be affected by the professional secrecy for information related to a whistleblowing case and also if exercising the rights above would hinder the investigation of a whistleblowing case. The possibility to exercise your rights will be assessed in light of the legal basis and purpose of the processing.

If you have any questions regarding the processing of your personal data, please contact us through the contact information provided in the beginning of this information.

Security

The company takes appropriate technical and organizational information security measures to prevent and limit risks associated with processing personal data, such as unauthorised access, disclosure, misuse, alteration, and destruction. Only authorized personnel bound by secrecy have access to identifiable personal data.