Information on processing of personal data in internal reporting channel for whistleblowing

Snusbolaget Norden AB ("**Snusbolaget**", "**we**", "**us**", and "**our**") processes personal data in our internal reporting channel for whistleblowing as further described in this information.

The internal reporting channel has been established in order to make it possible for reporting persons to report breaches under the Act on Protection of Persons who Report Wrongdoings (2021:890) (the "**Whistleblowing Act**") to the company.

Responsibility for the processing of personal data in the internal reporting channel

Snusbolaget is responsible for the processing of personal data in connection with managing the report in the internal reporting channel and any investigation carried out as a result of a report.

Snusbolaget has engaged the service provider NAVEX, which provides a secure web-reporting tool that can be used to submit reports. NAVEX is a processor in relation to Snusbolaget when NAVEX processes personal data on behalf of Snusbolaget for this purpose.

Additional information on the processing of personal data in the internal reporting channel

Personal data is collected from the reporting person that submits a report using the internal reporting channel, from other persons involved in the investigation of a report, from internal IT systems and, where applicable, from publicly available sources, for example information that is available online or from public authorities.

Please see below for additional information on the processing of personal data in the internal reporting channel.

Manage the internal reporting channel

Description: Personal data is processed to manage the internal reporting channel, including for collecting and assessing reports, communicating with individuals concerned, providing feedback to the reporting person, and carrying out investigations of a report, for example to assess whether any reported breach is accurate or not.

Categories of personal data:	Legal basis:	External recipients:
• Audio and video information • Breach information • Communication • Contact information • Employment information • Identity information • Matter information • Profile information	*Legal obligation* (Article 6.1 (c) of the GDPR) to fulfill the requirements under the Whistleblowing Act (2021:890). Identity information includes, where applicable, personal identity numbers, which are processed when necessary in order to securely identify the relevant person.	1. External counsel and expertise

Storage period: Personal data is stored for his purpose during the period the matter is active and for a period of up to two years after the matter was closed.

Reports submitted to the internal reporting channel, but which do not include breaches under the Whistleblowing Act, is stored for a period of four (4) months following the date when the person was notified of the decision not to investigate the report.

Follow-up and evaluate the internal reporting channel

Description: Personal data is processed in order to follow-up and evaluate the internal reporting channel, for example to create reports with statistics on how many reports that have been submitted during a specific period.

Categories of personal data:	Legal basis:	External recipients:
• Matter information	*Legitimate interest* (Article 6.1 (f) of the GDPR). The processing is necessary to satisfy our legitimate interests of following-up and evaluating the internal reporting channel. The assessment is that this legitimate interest outweighs your right to not have your personal data processed for this purpose, given the purpose of the processing and the limited impact that the processing implies, given that the result of the processing constitutes statistics which do not include any personal data.	Personal data is not shared with any external recipients that are separate controllers for this purpose.

Storage period: Personal data is stored for his purpose during the period the matter is active and for a period of up to two years after the matter was closed. Reports with statistics on an aggregated level are stored until further notice.

Manage, defend and exercise legal claims

Description: Personal data is processed to manage, defend and exercise legal claims as a result of a report, for example to file a police report or another notification with a public authority, to take legal measures against the person subject to a report or another person involved in the matter or to defend the business against legal claims for alleged breaches of law, including the Whistleblowing Act.

Categories of personal data:	Legal basis:	External recipients:
The same categories of personal data that are outlined above and which are processed in connection with the management of the internal reporting channel and will, where	*Legitimate interest* (Article 6.1 (f) of the GDPR). The processing of personal data is necessary to satisfy our legitimate interests of	1. Counterparty 2. External counsel 3. Relevant public authorities 4. Courts of law 5. Arbitration tribunals

necessary in the specific case, be shared with the relevant external recipients (1–7).	managing, defending, and exercising legal claims in a specific case. The assessment is this legitimate interest clearly outweighs your right to not have your personal data processed for this purpose, given the purpose of the processing.	6. Trade unions 7. Insurance companies

Storage period: Personal data is stored for this purpose for the time period that is necessary in order to manage, defend and or exercise the legal claim in the specific case.

Ensure the security of the internal reporting channel

Description: Personal data is processed to ensure the security of the internal reporting channel, for example to ensure that only authorized users have access to the web-reporting tool and in connection with logging and backups.

Categories of personal data:	Legal basis:	External recipients:
The same categories of personal data that are outlined above and which are processed in connection with the management of the internal reporting channel, in addition to: • Log information • Technical information	*Legal obligation* (Article 6.1 (c) of the GDPR) to implement appropriate technical and organizational security measures according to Article 32 of the GDPR.	Personal data is not shared with any external recipients that are separate controllers for this purpose.

Storage period: Personal data is stored for the same period as stated in relation to each relevant purpose of the processing of personal data.

Personal data in logs for troubleshooting and incident management is stored for a period of up to two years from the date and time of the log entry.

Personal data in backups are stored for a maximum period of up to two years from the date of the backup.

Categories of personal data

Please see below for table with information on the categories of personal data that are processed in connection with the internal reporting channel with examples of types of personal data.

Category of personal data	Examples of types of personal data
Audio and video information	Audio and video recordings, pictures, images
Breach information	Type of breach, date of breach, reason for breach, description of the breach
Communication	Contents of e-mails, chats, text messages
Contact information	E-mail address, address

Category of personal data	Examples of types of personal data
Employment information	Type of employment, employment period, role and responsibilities
Identity information	Name, personal identification number, employee-ID
Log information	Date and time of log event, log entry, type of log event
Matter information	Type of matter, date of matter, status of matter
Profile information	Title, level, age, gender, qualifications, company or organisation that the individual works for, status (for example absence etc.)
Technical information	IP address, type of device, device identifier, version of browser and operating system, network identifier

Your rights

According to the GDPR you have certain rights in relation to the processing of your personal data. Given the purpose and the nature of the processing of personal data in the internal reporting channel and that the identity of the reporting persons and other individuals that are involved in a whistleblowing matter are protected by a statutory obligation of confidentiality, your rights under the GDPR may in practice be limited.

According to the GDPR, you have the right to:

- Request access (Article 15 of the GDPR) to (a copy of) your personal data,
- Request rectification (Article 16 of the GDPR) of your personal data if it is incorrect or incomplete,
- Request erasure (Article 17 of the GDPR) of your personal data, but this right does not apply when the processing is carried out to fulfill a legal obligation such as in this case,
- Request restriction (Article 18 of the GDPR) of your personal data,
- Request a copy of your personal data in a structured, commonly used and machine-readable format (data portability) (Article 20 of the GDPR), but this right does not apply in relation to processing of personal data in the internal reporting channel, since the processing is not carried out for the performance of an agreement with you or based on your consent, and
- Object to the processing of your personal data (Article 21 of the GDPR), but please note that this right does not apply when we process personal data to satisfy our legitimate interest of managing, defending and exercising legal claims or when we have compelling legitimate grounds of processing your personal data, for example to manage the internal reporting channel.

If you wish to exercise your rights in relation to the processing of your personal data, please contact us on the contact details outlined below. Please note that it normally takes one (1) month to respond to your request as of the date we received your request.

We do not carry out any automated individual decision-making in connection with the processing of personal data in the internal reporting channel.

Your personal data is processed and stored within the EU/EEA.

If you have questions

If you have questions or concerns regarding the processing of personal data in the internal reporting channel, please contact us on the contact details outlined below. You always have the right to make a complaint with respect to the processing of your personal data. In Sweden, complaints are submitted to the Swedish Authority for Privacy Protection (IMY) (www.imy.se).

Snusbolaget Norden AB
Reg. no.: 556801-3683
Address: Östgötagatan 12, 116 25 Stockholm
E-mail: privacy@hayppgroup.com