Whistleblowing Privacy Notice

Document Information	
Name	Whistleblowing Privacy Notice
Effective from date	01.01.2025

This Whistleblowing Notice explains how personal data is collected, processed, and protected when you report concerns related to unlawful, unethical, or improper conduct within our legal entity or our clients.

SK in this Whistleblowing Notice stands for SK ID Solutions AS (registry code 10747013), SK ID Solutions AS filiāle Latvijā (registry code 40203201750) and SK ID Solutions AS Lietuvos filialas (registry code 304977982).

Whistleblowing Privacy Notice applies in all countries where SK operates, in line with the SK Whistleblowing Policy.

Every SK`s employee, trainee, volunteer, apprentice, contractor, consultant, applicant, shareholder, member of the management, administrative or supervisory board member, legal representative, partner, supplier, business contact must read this Whistleblowing Privacy Notice before reporting wrongdoings.

Important note: Speaking-up about wrongdoings, although encouraged by SK, remains purely voluntary. If your report contains personal data of yourself or others, please make sure it is limited to what is necessary to understand or resolve the case.

What concerns can you raise?

You can raise a compliance concern if you reasonably suspect a breach of laws, policies, and/or other SK`s obligations.

The nature of compliance concerns could include but are not limited to fraud, abuse, environmental issues, bribery, other breach of law or any other topic addressed in the SK`s Whistleblowing Policy. To assist in the investigation, those reporting potential violations are encouraged to identify themselves.

1. Who is responsible for your personal data

SK (“we”, “us”, “our”) will as data controller operate SK`s Whistleblowing solution to ensure that you know how to raise a compliance concern if you observe or suspect a wrongdoing and provide a remediation framework for serious and sensitive compliance concerns that could have an adverse impact on SK`s business.

2. Personal data we process

Below you will find a description of the personal data we will collect and process about you as well as the purpose on which basis we are processing the personal data when you use the Whistleblowing line.

In principle, the Whistleblowing line can be used, to the extent permitted by law, without providing your personal data. You may, however, voluntarily disclose your personal data as part of the Whistleblowing process.

Processed Personal data will generally be limited to:

- identity, location and contact details of the reporting person (if the report mentions such information).
- Whistleblowing report data: information related to the reported issue, including the nature of the alleged misconduct, unlawful activity, or regulatory breach.
- Third party data: personal data of individuals mentioned in the report (e.g., employees, contractors, or other stakeholders).
- Actions to be taken/already taken in relation with people mentioned in the report to either protect them and/or stop the wrongdoings.
- Special categories of data: In principle, we do not request or process any special categories of personal data (also known as sensitive personal data), e.g. information on racial and/or ethnic origin, religious and/or ideological convictions, trade union membership or sexual orientation. Due to free format of the reporting, however, such special categories of personal data may be voluntarily disclosed by you. Please do not reveal any sensitive personal data about yourself or anyone else if not strictly necessary for us to understand or resolve the case or protect you.

In any case, only personal data strictly necessary to understand, verify, clarify, and resolve reported facts will be processed. Personal data mentioned in unsubstantiated or out of scope reports or which are simply not necessary will be deleted and not considered if sensitive.

3. Purpose of the processing and the legal grounds

SK processes personal data to manage in a safe and efficient manner all reports of wrongdoings made under the Whistleblowing Policy – which includes the:

- analysis, storage and follow up of reports including exclusion of irrelevant reports
- investigation of reported facts (where relevant)
- necessary actions to stop the wrongdoings, preserve evidence and defend SK`s rights and assets
- protect the privacy, rights and safety of the reporting person, witnesses and third parties mentioned in the report as well as the rights of the accused person.

Processing Personal data for the management of reports is based on:

- a legal obligation – to provide safe reporting channels to the personnel and business contacts. This legal obligation exists within the EU/EEA, based on their national legislation implementing the EU Directive about Whistleblowing, and in many other countries across the world;
- a legitimate interest of SK to give the possibility to our personnel and business contacts to speak up and report wrongdoings and for us to receive and investigate whistleblowing reports to ensure a lawful and compliant way to make business;
- the necessity, in extreme cases, to protect the vital interests of the reporting person or other persons;
- in residual cases, where sensitive personal data is provided in a report, consent is the legal ground, as reporting is voluntary as well as the provision of any personal data in there. If not necessary to the resolution of the case, it will be immediately deleted.

4. How we process personal data

SK is using a third-party service provider Grant Thornton Baltic OÜ for our online Whistleblowing platform where the reports are hosted and managed.

5. Security, disclosure of personal data and international transfer of personal data

SK operates internationally and has locations in various countries within the European Union. The stored data may only be processed by specially authorised persons within SK. All persons authorised to inspect the data are expressly obliged to maintain confidentiality.

SK may also transfer your personal data to our external attorney or auditor in connection with the processing of the concern, including reporting the concern to relevant authorities, if necessary, and the police and/or courts in case of criminal investigation or lawsuit, local competent public authorities.

The board members, legal representative, line manager and HR department of the employer will be informed of the identity of the accused person only if wrongdoings are proved as well as the liability of the accused person, for the employer to take any necessary measures towards the concerned accused person. Works council will also be informed, if legally required.

We do not transfer personal data outside of the European Economic Area (EEA). If such a transfer becomes necessary, we will ensure that appropriate safeguards are in place, in accordance with GDPR, to protect your personal data.

6. Duration of storage

Personal data related to whistleblowing reports will be retained only for as long as is needed to fulfil our purposes of investigating compliance concerns and documenting our compliance with applicable laws, unless we are required under applicable law to keep your personal data for a longer period.

Different retention periods apply if legal proceedings or disciplinary measures are initiated.

The general principles are that: (i) only relevant personal data is kept, and (ii) personal data is not retained longer than necessary to fully manage a report (i.e. understand and analyse a report, investigate where necessary and resolve the concerned issue, which may include actions before courts and/or disciplinary actions).

More precisely, please note that:

- irrelevant reports (i.e. out of scope of the reporting policy or unfounded) or irrelevant personal data are archived immediately and deleted within three (3) years from the closing of investigation.
- reports for which no judicial or disciplinary procedure is necessary are deleted within three (3) years from the end of the verification/ investigation phase.
- reports leading to a litigation/disciplinary procedure are deleted once all statute of limitation periods have expired.

7. Which rights you have regarding your personal data

7.1. Reporting person

The privacy, rights and safety of the reporting person are ensured from the moment you make a report in good faith and during the entire reporting procedure.
If you are the reporter, you have the right to:

- The right to information and access – to know which personal data SK holds about you, obtain detailed information about how your data is used and who has access to it, you can obtain a copy of all your personal data, obtain its correction or rectification if incorrect or incomplete. There are some exemptions, which means you may not always receive all the personal data that we process, e.g. when there is an ongoing legal investigation.
- The right to object – you have the right to object to SK`s processing (using) your personal data. This effectively means that you can stop or prevent us from using your personal data. However, it only applies in certain circumstances, and we may not need to stop the processing of your personal data if we (i) have compelling legitimate grounds to process it that override your rights and freedoms, (ii) needs it to establish, protect or defend our rights or (iii) comply with applicable law.
- The right to erasure – you have the right to ask us to erase your personal data in certain circumstances provided that SK does not have to keep it for legal reasons.
- The right to rectification – you can also request SK to stop using your personal data until clarification (but not delete it), if you consider that your personal data have been used in violation of applicable data protection law. If you want to obtain any rectification, you can contact the respective member of the Compliance team via the Whistleblowing platform. You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete personal data you think is incomplete.
- The right to restriction of processing – you have the right to ask us to restrict the processing of your personal data in certain circumstances.

7.2. Accused person

If you are the accused person, you have the right to:

- information and access – be informed of the reported accusations against you, within six (6) months maximum from receipt of a report. By exception, when such notification may seriously jeopardize the efficiency of the investigation, the protection of evidence or the entire reporting process, it must be provided as soon as those risks do not exist anymore.
- erasure – require the deletion or correction of any incorrect personal data about you (you will be able to exert these rights once informed about the reported accusations).
- object – you do not have the right to object to the use of your personal data, except if you demonstrate that the reported facts are inexistent or do not involve you, or if the concerned personal data are incorrect or unnecessary to the resolution of the case.

If you are the accused person, you have the right for your reputation, privacy protected, and identity kept confidential by those in charge of managing the reports as long as the liability of you is not proved. In this context, the identity of the accused person cannot be revealed to the line manager, legal representatives and board members of the employer of the concerned accused person, as long as the liability is not proved.

7.3. Witnesses and any other person mentioned in the reports

If you are a witness or other third party mentioned in a report, you have the right to:

- The right to information and access – to know which personal data SK holds about you, obtain detailed information about how your data is used and who has access to it, you can obtain a copy of all your personal data, obtain its correction or rectification if incorrect or incomplete. Also to have your identity protected and kept strictly confidential by SK and not revealed to anyone without your express prior consent, provided that the disclosure of your identity to local authorities or courts is not required by applicable law.

- The right to object – object to the use of your personal data based on legitimate interests or consent, for reasons linked to your personal situation, and in that case SK will have to delete and stop using it except if it has an overriding legitimate interest to keep it, as a legal obligation or the necessity to protect the vital interest of someone; Object to the use of your personal data, based on grounds linked to their personal situation that would overweight the legitimate interest of SK.
- The right to erasure – request the deletion of your personal data provided that SK does not need to keep it anymore for legal reasons. You can also request SK to stop using your personal data (but not delete it) until clarification before a court or supervisory authority, if you believe that your personal data have been used in violation of applicable data protection law.

The right to complaint – anyone, whose personal data is processed, has the right to complaint (including the reporter, the accused person and the witnesses or any other person mentioned in the reports). If you have any complaints about SK`s processing of your personal data, please contact our Data Protection officer by simoona.hion@skidsolutions.eu.

If you are not happy with the way we handle your complaint, you may contact the respective Data Protection Authority.

8. Contact information

If you observe or suspect breach of laws, policies, and/or other SK`s obligations, you should report the compliance concerns through SK`s Whistleblowing line.

If you have any questions or concerns about how we process your personal data, please contact us by email: dpo@skidsolutions.eu regarding your personal data.

9. Changes to the Privacy Notice

We may need to change this Privacy Notice from time to time to ensure it meets the possible changes in the process or the updated laws. When changes are made, we will update the "Last Updated" date at the top of this notice and communicated it in our Whistleblowing platform.