



SOL Group

Policy on Reporting and Handling Misconduct and
Protecting Reporting Persons
(Whistleblowing Policy)



Table of Contents

1. Purpose and Scope	3
2. Channels for Reporting Ethical Concerns	3
2.1. Available Reporting Channels	3
2.2. Whistleblowing Reporting Channel	4
2.3. What Matters May be Reported?	4
3. Handling Reported Concerns	5
3.1. Key Principles for Handling Reported Concerns	5
3.2. Handling Reports	6
3.3. Assessment of Reports	6
3.4. Internal Investigation	7
3.5. Decisions Based on the Findings of the Investigation	8
4. Protection of Reporting Persons	8
4.1. Protection Against Retaliation	8
4.2. Definition of Retaliation	8
4.3. Requirement of Good Faith	8
4.4. Consequences of Retaliation	9



1. Purpose and Scope

The purpose of this Whistleblowing Policy (the “Policy”) is to define the principles and procedures applied by the SOL companies in situations where an employee or a third party wishes to report suspected misconduct or other action that is not in accordance with SOL’s principles of good business conduct, values or internal guidelines. Additionally, the Policy describes the operating model of the SOL companies for investigating reports and potential misconduct, as well as SOL’s commitment to protecting reporting persons.

The Policy aims to ensure transparent, independent and reliable procedures for reporting and investigating concerns and misconduct, and to safeguard the interests of reporting persons, people concerned by reports and the SOL companies.

The purpose of the guidelines is to encourage and enable employees and other stakeholders to raise concerns with the SOL companies, enabling the company to address inappropriate conduct and improve its operations. Speak Up reports shall always be handled without undue delay and in accordance with this Policy.

All business units and companies of the SOL Group and all directors, salaried employees and employees must comply with this Policy. In accordance with the EU Whistleblower Protection Directive and the national laws and regulations implementing it, this Policy may be supplemented by country-specific guidelines.

SOL’s Legal Department in Finland has central responsibility for monitoring and implementing compliance with this Policy and for responding to related questions. For SOL’s international companies, primary responsibility for monitoring and implementing compliance with the Policy rests with the people specifically designated by the relevant SOL company in the country concerned.

2. Channels for Reporting Ethical Concerns

2.1. Available Reporting Channels

At SOL, our objective and established way of working is to develop our business openly and in an ethically sustainable manner. Our employees, customers and other business partners are our most important sources of information. It is important that everyone reports suspected misconduct or conduct that is inconsistent with SOL’s principles of good business conduct, values or internal guidelines. This enables us to correct, prevent or remedy concerns and misconduct.

We provide several channels for raising and reporting identified concerns:

1. The first option is always to consider whether the situation could be resolved through discussion, questions and timely intervention. Raise the matter if something concerns you or you feel that something is not being handled properly. Matters can often be resolved at an early stage once they are brought forward for discussion.
2. You may always contact your supervisor and seek guidance, including when you are unsure about the appropriate course of action.
3. If you are unable or unwilling to contact your supervisor, or if you wish to report your supervisor’s conduct, you may contact your supervisor’s supervisor, an employee representative, an occupational safety and health representative, Human Resources department or SOL management.
4. You may also seek advice from the Legal Department or report the matter directly to the Legal Department. The Legal Department shall assist in assessing the situation and provide confidential guidance.
5. If, for any reason, the above options do not feel suitable, you may report your concern through the Whistleblowing reporting channel (see section 2.2). This channel is also available to external stakeholders.

In situations falling within the scope of the Finnish Whistleblower Protection Act¹, a report may, subject to certain conditions, also be made in Finland through the centralized external reporting channel maintained by the Office of the Chancellor of Justice. We encourage reporting primarily through internal channels. The external channel may be used

¹ The scope of application of the Whistleblower Protection Act (1171/2022) covers breaches detected in a work-related context within certain areas defined under EU law. A more detailed list of the areas falling within the scope of the Act can be found on Finlex: Whistleblower Protection Act (1171/2022), Section 2 (Scope of Application). Guidance on the use of the centralized external reporting channel is available on the website of the Office of the Chancellor of Justice.



where the reporting person is unable to use the internal whistleblowing reporting channel or has reasonable grounds to believe that the breach cannot be effectively addressed on the basis of an internal report or that the reporting person is at risk of retaliation. The centralized external reporting channel of the Office of the Chancellor of Justice is available at: [Centralised external reporting channel – the Office of the Chancellor of Justice | Chancellor of Justice](#)

2.2. Whistleblowing Reporting Channel

The Whistleblowing reporting channel is an early-warning system available to SOL employees and stakeholders. It is intended to help prevent misconduct and reduce risks to the company. The reporting channel, which is maintained by an independent third party, helps us promote compliance with our principles of good business conduct and maintain the trust of our customers and other stakeholders.

Through the channel, employees and third parties, such as job applicants, customers and business partners, are able to securely report identified concerns and, if they choose, do so anonymously to the extent permitted by local legislation. Section 3.1 explains what confidentiality, security and anonymity mean in this context.

The Whistleblowing reporting channel is available on the intranet home page and on the official external website of the SOL companies. The address of the reporting channel is: <https://report.whistleb.com/en/sol>

The Whistleblowing reporting channel is available in approximately 20 languages. A reporting person may nevertheless submit a report in any language.

To facilitate the effective handling of reports, reporting persons are encouraged to describe the concern in as much detail as possible and, where known, to provide the date(s) and location of the events.

Reports may be submitted anonymously, although reporting persons are encouraged to report under their own name. The identity of a reporting person shall be treated confidentially and disclosed only to those who are authorized, by virtue of their duties, to handle reports (see section 3.1). A reporting person submitting an anonymous report may, if they choose to do so, provide an email address anonymously to follow the progress of the report and receive possible requests for further information. The email address is not visible to the provider of the Whistleblowing reporting channel or to the people handling reports.

2.3. What Matters May be Reported?

SOL employees and external stakeholders may use the reporting channels referred to in section 2.1 to raise concerns or suspicions regarding conduct that breaches our principles of good business conduct, values or internal guidelines and may have serious consequences for SOL, SOL's customers, partners or individual people. Regardless of the channel used, SOL is committed to handling all reports in accordance with the procedures described in this Policy. Supervisors are required to refer any reported concerns involving a breach of SOL's principles of good business conduct to SOL's Legal Department.

The concerns described above may include, for example, the following. The list is not exhaustive:

- Breaches of legislation, regulatory requirements or internal guidelines applicable to SOL's business operations
- Financial misconduct, such as embezzlement, fraud or other improper financial conduct
- The offering, receipt or solicitation of bribes, and other forms of corruption
- Conflicts of interest or concealment of such conflicts
- Labour exploitation, harassment or discrimination
- Serious failures relating to occupational safety or occupational health
- Breaches of data protection or information security
- Unethical conduct in relation to customers, business partners or public authorities
- Serious environmental breaches or failures
- Retaliation against a reporting person or attempts to prevent reporting

The Whistleblowing reporting channel is not intended for reporting operational issues or concerns relating to terms and conditions of employment. Such matters should be handled through ordinary processes unless they involve suspected breaches of SOL's principles of good business conduct. Nor should the channel be used in emergencies involving an immediate threat to life, health or property.



A reporting person must act honestly and in good faith and have reasonable grounds to believe that the report is accurate. The reporting person is not required to present evidence of the suspected breach. However, to facilitate the investigation, the reporting person is encouraged to submit any available evidence with the report.

The reporting channels must not be used to make unfounded or false allegations. Employees who intentionally submit such reports may be subject to disciplinary action. A reporting person who raises a concern in good faith shall not be subject to disciplinary action even if the investigation does not establish any breach or misconduct.

3. Handling Reported Concerns

3.1. Key Principles for Handling Reported Concerns

All concerns are taken seriously

All concerns raised through the channels described above are taken seriously and handled professionally. Allegations of breaches of SOL's principles of good business conduct are investigated carefully and without undue delay. Necessary and appropriate action shall be taken to address any identified concerns.

Role of Supervisors

Supervisors are to act as the primary points of contact for employees when concerns are raised, providing support and answers to questions within the scope of their role. Supervisors must not personally investigate suspected misconduct where they cannot act impartially. Such situations may, for example, include investigating potential misconduct or inappropriate behaviour involving their own subordinate, unless the matter is an ordinary employment-related issue. Supervisors are required to refer reports requiring an independent investigation to the Legal Department.

Confidentiality

All reports are handled confidentially. The identity of the reporting person is disclosed only to persons who are authorized, by virtue of their duties, to handle reports submitted through the Whistleblowing Reporting Channel or to take part in the investigation process or the following proceedings.

Confidential handling means that the matter is investigated on a strict need-to-know basis and information is shared only to the extent required by the investigation. In some cases, including investigations concerning harassment or inappropriate treatment, all parties must be heard. In such cases, the identity of the reporting person may become indirectly apparent during the investigation even though the reporting person's name is not disclosed.

Anonymity

You may submit a report anonymously through the Whistleblowing reporting channel. In practice, this means that you do not provide your name when submitting the report. The Whistleblowing reporting channel has been designed so that your identity is not transmitted to the person handling the report through your IP address or through other indirect information. A reporting person submitting an anonymous report may, if they choose to do so, provide an email address anonymously in order to follow the progress of the report and receive possible requests for further information. The email address is not visible to the provider of the Whistleblowing reporting channel or to the people handling the reports.

However, we encourage everyone to report under their own name, as this facilitates follow-up questions and supports the investigation. Reporting under your own name is as secure as anonymous reporting because your identity shall be treated confidentially.

If a report concerns a criminal offence or another breach of law, it may be necessary to refer the matter to the competent authorities. In that event, anonymity cannot always be guaranteed, and the applicable procedure shall be determined by legislation. In some countries, anonymous reporting may be restricted or prohibited for certain categories of matters.

Security and data protection

The Whistleblowing reporting channel is secure, and its technical maintenance is provided by an external service provider. Information submitted in a report is handled confidentially in accordance with SOL's internal guidelines and applicable data protection legislation.



Personal data relating to reports is retained only for as long as it is necessary to handle and investigate the report or as required by law. When the data is no longer required, it shall be deleted or anonymized in accordance with applicable requirements and guidelines issued by the legal department in Finland.

3.2. Handling Reports

People Responsible for Handling Reports Submitted Through the Whistleblowing Channel

SOL's Legal Department in Finland has overall responsibility for handling the Whistleblowing reports concerning SOL's Finnish companies within the system and has access to the system to the extent required by its duties. This overall responsibility includes authority to investigate the accuracy of reports at all organizational levels and, where necessary, to assign the investigation to other designated SOL employees who have the appropriate qualifications. The person handling the report may also assign the investigation to an external expert. Reports concerning SOL's international companies are primarily referred to the persons specifically designated in the relevant country.

Impartiality

Any person involved in handling a report and investigating its accuracy within the SOL companies must be impartial. Conflicts of interest relating to the report or the person concerned by the report are not permitted. People involved in handling a report must recuse themselves and refrain from participating if their relationship with the matter or the parties could compromise their impartiality. A person removed on grounds of a conflict of interest shall not participate in the handling of the matter, and further handling of the report shall be transferred to an impartial person.

Timeline

All reports of serious concerns made in good faith through any reporting channel shall be investigated without undue delay.

The following time limits apply to reports submitted through the Whistleblowing reporting channel:

- The person handling the report shall send an acknowledgement of receipt to the reporting person within **seven (7) days** of receipt of the report.
- Reports shall be classified (see section 3.3).
- Feedback shall be provided to the reporting person within **three (3) months** of the acknowledgement of receipt. Whenever possible, the person handling a report shall inform the reporting person that the investigation has been completed and, where appropriate, that corrective action will be taken.
- The report is available to the reported for **four (4) months** from the date of sending the acknowledgement of receipt to the reporter.

Unfounded reports

The reporting channel must not be used maliciously or based on information known to be incorrect. When the reporting procedure is misused by knowingly making unfounded allegations, SOL may take appropriate action, which may include disciplinary consequences.

3.3. Assessment of Reports

Allegations made in reports are investigated in accordance with our predefined process by the designated people and, where necessary, with the support of designated internal or external experts. Both internal resources of the SOL companies and external resources may be used in an investigation.

The measures used to determine the accuracy of a report are defined on a case-by-case basis and may include, for example, reviewing documents and/or emails, conducting research and interviews.

Preliminary Assessment of a Report

Upon receipt of a report or observation, the person handling the report shall assess its validity and credibility without undue delay. The assessment shall consider whether the situation may involve a breach of applicable law, regulatory requirements, the internal guidelines of the SOL companies or the principles of good business conduct. When necessary, a responsible person with the requisite authority and competence shall be designated to conduct the preliminary assessment and determine the appropriate course of action, including whether to initiate an internal investigation.



Classification, Notification and Confidentiality

Once the nature and scope of the report or observation have been determined, the report shall be classified and a decision on further handling shall be made without delay. The person handling the report shall decide the handling process on a case-by-case basis, choosing at least from the following options:

1. No further action under this Policy is required, (for example because the report is unfounded, falls outside the scope of the channel or does not contain sufficient information to initiate further action). The reporting person shall be informed of the decision and, when possible, advised of an alternative channel.
2. The matter is referred to the director responsible for the relevant business or Human Resources for further handling (for example when the nature of the report falls outside the Whistleblowing procedure and instead concerns operational management or ordinary HR processes).
3. It is justified to initiate a formal internal investigation (see section 3.4).

The necessary representatives of the SOL companies, (such as the Managing Director, business directors, HR management, financial management and/or a representative of the Board of Directors), shall be informed without delay of significant reports, particularly when a report concerns suspected (i) financial misconduct, (ii) a material breach of internal guidelines or the principles of good business conduct, or (iii) a material reputational or publicity risk is related to the matter. If the report concerns management, information shall be provided in a manner that avoids conflicts of interest and safeguards the impartiality of the handling process.

The identity of the reporting person shall be kept confidential, and information shall be shared only with people who have a justified need to know for the purpose of handling the matter. The people handling reports and those participating in the investigation are required to keep the contents of the report confidential unless disclosure is necessary to investigate the matter or comply with a legal obligation. In some cases, including investigations concerning harassment or inappropriate treatment, all parties must be heard. In such cases, the identity of the reporting person may become indirectly apparent during the investigation even though the reporting person's name is not disclosed.

3.4. Internal Investigation

If the persons handling the reports decide to initiate an internal investigation, the following principles shall, at minimum, be observed:

1. The member of management relevant to the investigation shall be identified and informed that the investigation has been initiated, subject to applicable confidentiality obligations.
2. Other persons who need to be informed of the investigation shall be identified, including the person concerned by the report where such notification does not compromise the investigation.
3. A person or team responsible for the internal investigation shall be appointed. The investigator or team must have the necessary competence and be demonstrably impartial. If an impartial internal investigation cannot be arranged, an external expert may be engaged.

The independence and impartiality of the persons carrying out the internal investigation and the investigation tasks shall be ensured and documented for each investigation. The report giving rise to the investigation, as well as information and material collected during the investigation, shall be disclosed only to persons with a justified need to know.

All persons participating in the investigation must keep all information received during the investigation confidential. The investigation findings shall not be published or discussed with anyone other than persons with a justified need to know. Confidential handling is important in order to protect privacy and safeguard the rights of the reporting person and the persons concerned by the report, as well as to ensure data protection, whistleblower protection and the appropriate handling of the matter.

The investigation must be documented in accordance with the guidance provided by the Legal Department.



3.5. Decisions Based on the Findings of the Investigation

If an investigation establishes that the principles of good business conduct or other guidelines of the SOL companies, or applicable law, have been breached, appropriate corrective and, where applicable, disciplinary measures shall be taken (including possible termination of employment). Such measures may also include criminal-law measures and any necessary corrective and preventive action to prevent similar misconduct from recurring.

As a rule, the relevant business is responsible for decisions on disciplinary and corrective measures based on the outcome of the investigation. The Legal Department, or the designated responsible person in an international SOL company, is responsible for carrying out an independent investigation to support decision-making and for ensuring, to the extent possible, consistency of measures across the organization.

4. Protection of Reporting Persons

4.1. Protection Against Retaliation

A person reporting suspected misconduct has a statutory right to protection against retaliation, provided that, at the time of reporting, the reporting person has reasonable grounds to believe that the information concerning the breach is true and that the information falls within the scope of the Finnish Whistleblower Protection Act (see footnote 1). A further condition for statutory whistleblower protection is that a report concerning a breach identified in SOL's operations is made primarily through SOL's Whistleblowing reporting channel.

In addition to the statutory whistleblower protection described above, the SOL companies are committed to ensuring that no person who, in good faith, reports suspected misconduct or other concerns, or participates in an investigation, is subjected to retaliation.

Submitting a report does not grant the reporting person immunity from measures that are based on legitimate grounds and are unrelated to the report. If the reporting person has participated in the suspected misconduct, reporting it does not release that person from possible employment-law, civil-law, criminal-law or regulatory liability. The SOL companies may nevertheless take into account that the reporting person voluntarily made the report in good faith and contributed to the investigation of the matter.

4.2. Definition of Retaliation

Retaliation means any disadvantageous measure or treatment directed at an employee or another person protected in connection with reporting, where the measure or treatment results from a report made in good faith or from participation in the investigation of a report.

Examples of retaliation include the measures listed below. The list is not exhaustive:

- Reduction of duties, responsibilities or status
- Suspension, lay-off or termination of employment
- Denial of promotion, training opportunities or pay increases because of reporting
- Unjustified disciplinary measures or other disadvantageous employment-related decisions
- Threats, pressure or other inappropriate treatment
- Discriminatory or hostile treatment or the creation of a hostile working environment
- Obstruction of work, isolation or damaging reputation
- Preventing or attempting to prevent reporting
- Breach of the confidentiality of a report or the identity of the reporting person

4.3. Requirement of Good Faith



The SOL companies do not tolerate any form of retaliation against a person who, in good faith, reports suspected misconduct or another concern or participates in the investigation of a report.

Good faith does not require the reporting person to be correct or to have substantial evidence supporting the concerns or questions raised. It requires only that the information provided has not been fabricated or intentionally presented in a misleading manner.

Reports that are intentionally misleading, unfounded or malicious may result in disciplinary action.

4.4. Consequences of Retaliation

Preventing or attempting to prevent reporting, retaliating against a reporting person or breaching the confidentiality of a report violates SOL's principles and this Policy. Such conduct may result in disciplinary action, including termination of employment.