P Reporting (Whistleblowing) Policy

Entry into force:	17 December 2021
Document owner:	Head of Group Compliance
Approved by:	Board of Directors on September 20, 2021
Replaces the following document:	Whistleblowing Policy 31 December 2008
Contact person in the event of questions:	Head of Group Compliance

Table of Content

I. Purpose 2
II. Scope of Application 2
III. Policy Statement 2
IV. Definitions 2
V. Reporting and Disclosing of Information 3
1. Material Scope 3
2. Available Reporting Channels 4
2.1 Internal Reporting Channels 4
2.2 External Reporting Channels 4
2.3 Public Disclosure of Information 5
VI. Procedure on handling Reports (receipt and feedback) 5
VII. Protection 5
1. Reporting Person 5
2. Accused Persons 6
VIII. Transparency and Fairness 7
IX. Confidentiality 7
X. Data Protection 7
1. Affected data 7
2. Retention of Reports and Related Information 7
XI. Conflict with National Law 7

I. Purpose

At Oerlikon, we are committed to the highest levels of ethics and integrity in the way that we do business. We understand that this is crucial to our continued success and reputation. Our values, Code of Conduct, policies and directives, guide our everyday business conduct. The aim of this Policy is to better protect anyone who reports a Breach, e.g., Employees, trainees and persons in "worker-like" situations who have information about any wrong-doing in connection with their professional or official activities and who choose to report or disclose such information. Further, this Policy seeks to improve the structural conditions for reporting at Oerlikon ensuring the unhindered flow of information and the protection of "Reporting Persons" who report incidents of any wrongdoing, of those persons who are subject of such reporting and whose alleged misconduct has not been established beyond a reasonable doubt and of any Third Party mentioned in the report.

II. Scope of Application

This Policy applies to all Reporting Persons, Accused Persons and any third parties mentioned in Reports as defined by law, who need to be protected in accordance with applicable laws and regulations in the respective jurisdictions globally in which Oerlikon operates.

III. Policy Statement

The decision to report is a personal one and it is up to each individual to choose whether to come forward and to speak up about information of known or possible wrongdoing or unethical behavior.

Oerlikon strongly encourages all Employees to speak up about any suspected or witnessed matters of concern. All Reporting Persons are protected by applicable laws, legislations and our regulations in their respective jurisdictions. Oerlikon asks that Employees report actual or suspected breaches of e.g. (i) applicable laws, (ii) legislations and regulations, (iii) our Code of Conduct; and (iv) policies and other internal regulations underlying the Code of Conduct. Oerlikon takes all Reports made under this Policy seriously.

Oerlikon will not hinder reporting or retaliate, and prohibits its Employees from hindering, retaliating or threatening to retaliate against any Employee or Third Party who in Good Faith reports or intends to report concerns of actual or suspected Breaches as laid out above.

IV. Definitions

Accused Person: Anyone who is the subject of an alleged Breach, wrongdoing or misconduct.

Breach: Violations of applicable laws, legislations and regulations, our Code of Conduct and policies as well as other internal regulations underlying the Code of Conduct.

Data Protection: Refers to the protection of people's privacy and personal data. By Personal Data, we mean any information that may directly or indirectly identify an individual. Data

Protection laws are the laws and regulations relating to Data Protection, they are not limited to GDPR. Most countries where Oerlikon operates do have Data Protection laws and regulations.

Disclosure: Making information about Breaches available to the public.

Employees: Any person or representative working with the Oerlikon Group or any of its entities. This includes among other Employees, shareholders, persons belonging to the administrative, management or supervisory board, persons having self-employed status, trainees, volunteers, officers, contractors, subcontractors, suppliers, and their employee. For the purposes of this Policy, employee includes applicants and persons whose contracts of engagement have already ended or have not commenced yet.

Follow-up Actions: Actions taken by an internal reporting office or by an external reporting office to verify the validity of a report, to take further action against the reported violation, or to close the case.

Good Faith: Means that the Reporting Person has reasonable grounds to suspect that, in light of the circumstances and the information available to them at the time of Reporting, the information reported is true.

Information on Breaches: Shall be reasonable suspicions or knowledge of actual or possible violations, as well as of attempts to conceal such violations, which have already been committed or are very likely to be committed.

Reports: Communications of information on Breaches to internal reporting channels or external reporting channels.

Reporting Person: Anyone who reports or speaks up about a Breach.

Retaliation: Acts or omissions in connection with professional activity which are a reaction to a Report or Disclosure and as a result of which the person making the report or the Accused Person suffers or may suffer an unjustified disadvantage.

Third Party: Facilitators, legal entities that the Reporting Person owns, works for or is otherwise connected with in a work-related context or any person who could indirectly experience Retaliation including but not limited to colleagues or relatives of the Reporting Person who are also in a work-related connection with Oerlikon, or its customers and all other persons awarded according protection by the respective applicable laws.

V. Reporting and Disclosing of Information

1. Material Scope

Reporting Persons are encouraged to report and disclose information concerning any unlawful activity or misconduct to:

- violations that are subject to criminal penalties or fines in accordance with national jurisdiction,

- other violations of laws, statutory ordinances and other regulations in countries where Oerlikon operates,
- violations of directly applicable legal acts of the European Union,
- actual or suspected Breaches of our Code of Conduct and the underlying policies, directives and other internal regulations.

2. Available Reporting Channels

Available reporting channels may include but are not limited to (i) internal channels within the company or (ii) any external reporting channels depending on the legitimate legal legislation in the jurisdiction in which Oerlikon has its commercial entity and the country in which the alleged unlawful activity or misconduct has taken place.

Employees who intend to report a Breach may choose between an (i) internal reporting channel within the company or (ii) an external reporting channel, in accordance with the applicable law of the country of the Oerlikon entity to which the Reporting Person belongs.

2.1 Internal Reporting Channels

Oerlikon recommends using its internal reporting line “Speak-Up” service to report discovered or imminent Breaches. While Oerlikon’s reporting line is the preferred channel, a Report can also be made directly to:

- a supervisor;
- a responsible Human Resources manager;
- the Compliance and Legal Departments;
- a respective Group representative of Group Compliance or Group Legal responsible(s);
- any other representative responsible for specific tasks, e.g., in HSE, Controlling Finance

Reporting Persons have the opportunity to submit Reports either in writing via online measures such as via email, or by post and/or verbally via the company’s reporting line “Speak-Up” or answering system. If requested by the Reporting Person, a face-to-face meeting is also possible. In all reporting channels, the confidentiality of the Reporting Person, the Accused Person and any Third Party mentioned in the Report will be protected according to the applicable laws.

Reporting Persons also have the possibility to submit Reports anonymously.

2.2 External Reporting Channels

We encourage everyone to report breaches directly and internally at Oerlikon as Compliance violations can jeopardize our core business values and high standards of ethics and integrity. Reporting Persons can report Breaches to the competent national authorities without having reported such Breaches internally first. Reporting Persons shall refer to the competent national authority’s website for information on how to report.

Information on external reporting channels can also be found by consulting the relevant local regulatory authorities.

2.3 Public Disclosure of Information

Depending on the specific national regulation according to public Disclosure of Breaches, persons who disclose information about violations publicly shall be subject to the protective measures of the respective law only if they:

1. filed an internal and external Report, and no appropriate action was taken following these Reports within the time limits for each Report; or
2. had sufficient reason to believe that (i) the violation may pose an immediate or obvious threat to the public interest, (ii) in the event of an external Report, Retaliation has to be feared, or (iii) due to the particular circumstances of the case, there is little prospect that the external reporting body will initiate effective follow-up measures.

VI. Procedure on handling Reports (receipt and feedback)

The Reporting Person will receive an acknowledgement of receipt within and no later than seven (7) business days of receipt of the Report.

The person(s)/team(s) responsible for Follow-up Actions will maintain contact with the Reporting Person and (i) check(s) the validity of the Report received, (ii) request(s) further information from the Reporting Person, if necessary; and (iii) communicate(s) Follow-up Actions.

The Reporting Person will get feedback within three (3) months of Oerlikon having acknowledged receipt of the Report or, if receipt has not been acknowledged, no later than three (3) months and seven (7) days after receipt of the Report.

The feedback will include notification of planned as well as already taken Follow-up Actions and the reasons for them. Where appropriate Follow-up Actions are still being determined, the Reporting Person will be informed about this and about further feedback to expect.

Feedback may be provided to the Reporting Person only to the extent that it does not affect internal inquiries or investigations and does not prejudice the rights of the Accused Person or persons who are named in the Report.

VII. Protection

1. Reporting Person

Oerlikon is committed to taking all reasonable steps to protect the Reporting Person or a Third Party from damages or abuse as a result of making a Report in Good Faith under this Policy and any recognized Reporting legislation.

Persons who reported or publicly disclosed information on breaches anonymously, but are subsequently identified and suffer Retaliation, nonetheless qualify for this protection, provided that they were in Good Faith.

Oerlikon does not tolerate any form of malicious or retaliatory conduct or attempted conduct taken by any person against the Reporting Person or anyone who is involved in an investigation of a Report. Examples of malicious or retaliatory conduct can include, but are not limited to:

- dismissal of an Employee or alteration of an Employee's position / duties to their disadvantage, or negative performance feedback that is not reflective of actual performance
- harassment, intimidation, or bullying;
- threats to cause detriment, including to reputation, e. g. in social media, or financial loss, including loss of business and loss of income;
- early termination or cancellation of a contract for goods or services.

Oerlikon takes all allegations of such conduct very seriously. If anyone is confronted or believes they are confronted with such conduct, it must be reported immediately so that an appropriate investigation can be initiated.

When making a Report, we expect the Reporting Person to be in Good Faith, i.e. to have reasonable grounds to suspect the information which will be disclosed is true. The Reporting Person will not be subject to any damage or abuse if the information turns out to be incorrect.

However, the Reporting Person must not make a Report if he/she/they know(s) it is not true or is misleading. Knowingly making a false Report is in any case not protected by this Policy, a violation of the Oerlikon Code of Conduct and may result in disciplinary action as well as legal consequences for the Reporting Person.

2. Accused Persons

The Accused Person shall be duly notified of the reported accusations within one (1) month. 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. This requires a case-by-case examination.

This notification must specify:

- the nature and content of the accusation(s); and
- the references to the protection of the person based notably on national constitutional rights; judicial, employment and Data Protection laws. This notably includes the (i) right of information, access, objection, correction and deletion of personal data (those rights however can't be exerted in order to obtain the deletion of an evidence or to change the reality of history and factual elements) and the right to (ii) comment on any accusation and defend her-/himself/themselves. The Accused Person has a right to a fair hearing and benefits from all employment rights applicable in a disciplinary procedure if she / he / they is an employee.
- the procedure and the names of the persons involved in the investigation.

VIII. Transparency and Fairness

Oerlikon ensures that in all Oerlikon Group companies, the reporting process is transparent and fair for all Employees, the Reporting Person and the Accused Person, and that their rights and privacy are respected.

IX. Confidentiality

Oerlikon ensures that the identity of the Reporting Person, witnesses or other involved persons, if any, shall remain undisclosed to anyone beyond the authorized staff members competent to receive or follow-up on Reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the Reporting Person may be directly or indirectly deduced.

X. Data Protection

1. Affected data

Personal Data will only be processed in compliance with applicable Data Protection and cyber security laws, in particular the General Data Protection Regulation (GDPR).

2. Retention of Reports and Related Information

Reports will not be stored longer than necessary and proportionate in order to comply with the requirements imposed by this Policy, or other requirements imposed by applicable laws.

Personal data in Reports out of scope of this Policy as well as personal data relating to Reports found to be unsubstantiated will be deleted immediately.

Personal data in Reports leading to a in the meanwhile completed investigation where no judicial or disciplinary procedure is required will be deleted within two (2) months from the end of the verification/ investigation phase.

In case the personal data in Reports is needed for purposes of specific further steps, e. g. a Report leading to civil or criminal litigation or disciplinary procedure, personal data will not be deleted as long as data storage is necessary for these purposes.

XI. Conflict with National Law

Mandatory national legal provisions, which contain conflicting or stricter requirements regarding particular aspects of this Policy, shall override the validity of these provisions. The Head of Group Compliance must be notified if a conflict with national law is identified.

Approved by the Board of Directors on September 20th, 2021.