

## Reporting Privacy Notice

### Introduction

The aim of this Reporting Privacy Notice is to ensure a high level of protection and transparency for all individuals whose personal data will be processed by Oerlikon (i.e. OC Oerlikon Management AG, Pfäffikon and its affiliates) in the frame of a Reporting process.

This Reporting Privacy Notice applies in all countries where Oerlikon operates, in line with our Reporting policies and is dedicated to any Oerlikon's employee, trainee, volunteer, apprentice, contractor, consultant, applicant, shareholder, member of the management, administrative or supervisory board, legal representative, partner, supplier, business contacts who would like to report a wrongdoing.

#### **Important notes:**

Reporting wrongdoings, if encouraged by Oerlikon, remains purely voluntary. You can report without mentioning your name or any other information about yourself in the report, if you wish. If your report contains Personal data, please make sure it is limited to what is necessary to understand and resolve the case.

Everyone has the possibility to use either the Speak- Up app, phone line or online platform to report wrongdoings to the Oerlikon Head of Compliance and Head of Internal Audit.

**Table of Contents**

- 1. Definitions .....3
- 2. Who will be responsible for Processing Personal data? .....3
- 3. What is the purpose for Processing Personal data? .....3
- 4. What are the legal grounds for Processing Personal data? .....4
- 5. Which categories of Personal Data will be processed and where the data will come from? .....4
- 6. What are the data protection rights of the Reporting person and other individuals mentioned in the Reports and which specific measures are in place to protect their privacy, rights and safety? .....5
  - 6.1 Reporting Person .....5
  - 6.2 Accused Person .....6
  - 6.3 Witnesses and any other person mentioned in the Reports .....6
- 7. Who will have access to this Personal data? .....7
- 8. Will your personal data be transferred overseas? .....7
- 9. Will Oerlikon make use of automated decision making? .....8
- 10. How long will your Personal Data be retained by Oerlikon? .....8
- 11. Are your data safe and secure?.....8
- 12. Changes to the Privacy Notice .....9

## 1. Definitions

**Processing:** means any operation or set of operations performed on Personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Personal data:** means any information that may, directly or indirectly, identify an individual.

**Sensitive Personal data:** is any Personal data which, if misused or accessed by unauthorized people, may have serious consequences for the rights, safety, freedom of individuals. Which Personal data is considered sensitive must be analyzed based on the laws of the country where the legal entity Processing this data is located, as the notion of sensitive Personal data varies from a country to another. Within the EU/EEA, UK and Switzerland, are expressly considered sensitive: Personal data revealing racial or ethnic origin; political, religious and philosophical beliefs and activities, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, intimate life (Switzerland), sex life or sexual orientation, but also criminal offences and sanctions, administrative and criminal judicial proceedings (Switzerland), social difficulties and measures of social assistance (Switzerland). Unique national identification numbers are considered sensitive in many countries across the Globe.

## 2. Who will be responsible for Processing Personal data?

When a case is reported through the Speak Up app, phone line or online platform : OC Oerlikon Management AG, Pfäffikon is legally responsible for the collection and processing of Personal data linked to the report jointly with the Oerlikon affiliate whose employee or external contact reported the wrongdoing .

When a case is not reported centrally through Speak up but directly to a local authorized person - as a supervisor or human resources person - as permitted by our Reporting Policy: the Oerlikon entity receiving directly the Report and dealing with the same- is legally responsible for the collection and use of your Personal data.

## 3. What is the purpose for Processing Personal data?

Oerlikon processes Personal data to manage in a safe and efficient manner all reports of wrongdoings made under the Reporting policies - 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 Oerlikon'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.

#### **4. What are the legal grounds for Processing Personal data?**

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

- a legal obligation<sup>1</sup>; to provide safe Reporting channels to the personnel and business contacts. This legal obligation exists e.g., within the EU/EEA<sup>2</sup>, based on their national legislation implementing the EU Directive about Whistleblowing, and in many other countries across the globe;
- a legitimate interest of all Oerlikon entities to give the possibility to their personnel, business contacts and stakeholders to speak up and report wrongdoings to ensure a lawful, ethical and fair way to make business<sup>3</sup>. It must be analyzed, on a case-by-case basis, whether the rights and interests of an individual, based on his personal situation for example, do not overweight the legitimate interest of Oerlikon to process his Personal data. For example, when the report covers facts of minor importance, it is relevant to promptly delete related Personal data in a report and not take them into account;
- the necessity, in extreme cases, to protect the vital interests of the Reporting person or other persons<sup>4</sup>;
- 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. Please think twice before revealing sensitive Personal data about yourself or anyone else if not necessary for us to understand or resolve the case or protect you;
- in countries leveraging exclusively on consent, consent may be used as legal ground given that the Reporting procedure is totally voluntary and individuals are not obliged to provide personal data given that anonymous reports are authorized.

#### **5. Which categories of Personal Data will be processed and where the data will come from?**

Personal Data Processed under the Reporting procedure will be limited to those:

- mentioned in the reports including any piece of information, evidence provided with the report or;
- resulting from investigations about reported facts.

In any case, only Personal data strictly necessary to understand, verify, clarify, and resolve reported Facts will be Processed. Personal data mentioned in unfounded or out of scope reports or which are simply not necessary will be promptly deleted and not considered, in particular, if sensitive.

Processed Personal data will generally be limited to:

- identity and contact details of the Reporting person (if the report mentions such information) and people mentioned in the report, relationship between Oerlikon and these people ;
- reported facts (suspected or witnessed);
- actions to be taken/already taken in relation with people mentioned in the report to either protect them and/or stop the wrongdoings.

However, the Reporting person can report without providing his/her name or any other information identifying her - when she reports through Speak up, she can let a message on the Speak- Up app, phone line or internet platform without any mandatory personal data being required. Any Reporting person using the Speak up phone line will receive an automated generated case number line so that she can follow up on her report, but this number is related to the Report not an individual. That is to say that no one can

---

<sup>1</sup> GDPR, article 6.1.c)

<sup>2</sup> e.g. Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law

<sup>3</sup> GDPR, article 6.1.f)

<sup>4</sup> GDPR, article 6.1.d)

identify the Reporting person thanks to this number. If the Speak app is used, the Reporting person can also remain anonymous and if she wants to see her report, she just needs to insert her 6-digit PIN code.

## 6. What are the data protection rights of the Reporting person and other individuals mentioned in the reports and which specific measures are in place to protect their privacy, rights and safety?

### 6.1 Reporting Person

The privacy, rights and safety of the Reporting person are ensured from the moment she makes a report in good faith and during the entire Reporting procedure.

First the security of the Report is ensured through technical measures .

- When the Reporting person uses the phone line or online platform to report:

she must keep strictly confidential and in a secure place the case number that she will receive from People Intouch when she will report online, as she will need that number to follow up on her report and request a copy of it. This case number must in no way be shared with others. This number does not enable People Intouch or Oerlikon to identify the Reporting person, it is related to a report not an individual.

- When using the Speak- Up app, the Reporting person will not receive a case number. She needs to create a PIN code once she downloads the Speak Up app, scan the QR code and insert the organisation code shared by Oerlikon to be able to leave a message in Speak- Up. After she leaves her message, she is informed that she will receive a reply within a week and the app asks her if she wants to receive push notifications.

The Reporting person has the right to:

- decide to report or not;
- report anonymously or not;
- receive an acknowledgement of receipt of her report within 7 working days (Monday to Friday);
- access and obtain a copy of the transcript or minutes of her report, obtain its rectification:
  - when the Reporting person uses the Speak Up system: she can exert that access right and read again her report by logging back into the Speak Up system (by using the individual provided case number or PIN code (for the app)).
  - If the Reporting person did not use the Speak Up system, she must contact directly the person to whom she reported directly the wrongdoings to exert her rights..
- know which Personal data Oerlikon holds about her, obtain detailed information about how her data is used and who has access to it, she can obtain a copy of all her Personal data, obtain its correction or rectification if incorrect or incomplete. The Reporting person can exert this right by sending an email either to the Head of Compliance if she reported through the Speak Up system or to the competent person to whom she reported wrongdoings;
- object to the use of her Personal data, based on grounds linked to her personal situation, except if Oerlikon (i) has compelling legitimate grounds to Process it that override the rights and freedoms of the witness (ii) needs it to establish, protect or defend its rights or (iii) comply with applicable law. The Reporting person can exert this right by sending an email to the Head of Compliance if she reported through the Speak Up system or to the competent person to whom she reported wrongdoings;
- have her identity protected and kept strictly confidential by Oerlikon even after closure of the case, provided that the disclosure of her identity to a competent authority or court is not required by applicable law;
- be protected by Oerlikon against any retaliation measure, every time she reports in good faith, and even if the reported facts are not correct at the end or not investigated or unfounded or out of scope of the Reporting procedure;

- request the deletion of her Personal data provided that Oerlikon does not have to keep it for legal reasons. She can also request Oerlikon to stop using her Personal data until clarification (but not delete it), if she considers that her Personal data have been used in violation of applicable data protection law;

The Reporting person can contact the Global Data Privacy and Data Compliance Officer (at [privacy.corporate@oerlikon.com](mailto:privacy.corporate@oerlikon.com)) for any concern in relation with the use of her Personal data in the context of a Reporting of wrongdoings. She also has the right to complain with the Swiss Federal data Protection and Information Commissioner (case managed reported through Speak-Up) and to her local data protection authority (case reported locally), if she believes that her Personal data have been misused during the Reporting procedure.

## 6.2 Accused Person

The Accused person has the right to:

- benefit from the presumption of innocence as long as her liability is not proved,
- be informed of the reported accusations against her, within 1 month maximum from receipt of a report<sup>5</sup>. 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 will require a case-by-case analysis. This notification must cover all information mentioned in the “Protection” chapter of the Reporting Policy;
- defend her rights and present her arguments once informed of the reported accusations and in any disciplinary procedure;
- get a copy of Personal data relating to her and require the deletion or correction of any incorrect Personal data about her (the Accused person will be able to exert these rights once informed about the reported accusations). She does not have the right to object to the use of her Personal data, except if she demonstrates that the reported facts are inexistent or do not involve her, or if the concerned Personal data are incorrect or unnecessary to the resolution of the case.
- have her reputation, privacy protected and her identity kept confidential by those in charge of managing the reports as long as the liability of the accused person 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 her liability is not proved.
- contact the Global Data Privacy and Data Compliance Officer (at [privacy.corporate@oerlikon.com](mailto:privacy.corporate@oerlikon.com)) for concerns in relation with the use of her Personal data. She also has the right to complain with the Swiss Federal Data Protection and Information Commissioner (case reported centrally through Speak-Up) or to her local data protection authority (case reported locally) if she believes that her Personal Data have been used in violation of applicable data protection law.

## 6.3 Witnesses and any other person mentioned in the report

The witnesses and other third parties mentioned in a report have the right to:

- decide to speak or not;
- have their identity protected and kept strictly confidential by Oerlikon and not revealed to anyone without their express prior consent, provided that the disclosure of their identity to local authorities or courts is not required by applicable law;
- know whether Oerlikon holds Personal data about them and how and why it is used and who has access to it;

---

<sup>5</sup> Article 14. 3.a ) GDPR.

- obtain a copy of their Personal data and obtain its correction or rectification, if incorrect or incomplete. They can also object to the use of their Personal data based on legitimate interests or consent, for reasons linked to their personal situation, and in that case Oerlikon 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 their Personal data, based on grounds linked to their personal situation that would outweigh the legitimate interest of Oerlikon and request the deletion of their Personal data provided that Oerlikon does not need to keep it anymore for legal reasons. They can also request Oerlikon to stop using their Personal data (but not delete it) until clarification before a court or supervisory authority, if they believe that their Personal data have been used in violation of applicable data protection law;
- contact the Global Data Privacy and Data Compliance Officer ([privacy.corporate@oerlikon.com](mailto:privacy.corporate@oerlikon.com)) for any concern in relation with their Personal data
- complain to the Swiss Federal Data Protection and Information Commissioner (case reported centrally through Speak-Up) or to their local data protection authority (case reported locally) if they believe that their personal data have been violated during the Reporting procedure or to their local data protection authority of the case was reported locally.

## 7. Who will have access to this Personal data?

Personal data will be accessible to:

- Oerlikon's external provider People Intouch: if you report through the Speak up app, phone line or online platform. People Intouch will receive the report and any related evidence /piece of information provided with the Report on behalf of Oerlikon. It will have, notably, to collect reports, transcript phone calls in writing, translate where necessary, upload and store all Reports in the Oerlikon's management space of its online platform and inform Oerlikon of those new reports;
- Oerlikon Head of Compliance and Oerlikon Head of Internal Audit if the Reporting person reports through the Speak Up app, phone line or online platform ;
- any person to whom the Reporting person would have decided to report directly, in line with the Reporting Policies (no use of Speak Up);
- any authorized Oerlikon employee or external counsel or expert asked by Oerlikon Head of Compliance or Oerlikon Internal Audit to provide assistance in the investigation, if any;
- 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 and findings only if wrongdoings are proved as well as the liability of the accused person, in order for the employer to take any necessary measures towards the concerned accused person. Works council will also be informed if legally required.

## 8. Will your personal data be transferred overseas?

The Reports sent through the Speak up phone line or online platform are stored within the EU by the supplier of the Speak Up (People Intouch) and are then managed by the Head of Internal Audit and Head of Compliance who are both working at OC Oerlikon Management AG, Switzerland.

Exceptionally, the data may be accessed from overseas by the abovementioned stakeholders or be transferred by them outside of the EU/EEA or Switzerland (i) where necessary for the investigation; (ii) where it is legally required to disclose it to local authorities and courts or (iii) where it is absolutely necessary to protect vital interests of people.

At Oerlikon, we have an Intra Group Data Transfer and Processing Agreement (IGDTPA) that protects Personal data transferred overseas within the group and is based on the Standard Contractual Clauses of the European Commission.

#### **9. Will Oerlikon make use of automated decision making?**

No. No software or technology dictates or influence our decisions. Software, online platforms, are just tools used to store and classify relevant information. No system providing automatic decisions or scoring is used. Oerlikon bases all its actions on human decisions, taken thoroughly, based on objective elements of proof, analysis of risks, applicable laws, our Code of Conduct, the presumption of innocence, the right to a fair trial, data privacy and employment law principles as fairness, transparency, data accuracy and with the safety of our people in mind.

#### **10. How long will your Personal Data be retained by Oerlikon?**

The general principles are that: (i) only relevant Personal data is kept, (ii) Personal Data is not retained longer than necessary to fully manage a report (i.e. understand and analyze 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 Policies or unfounded) or irrelevant Personal data are deleted immediately.
- reports for which no judicial or disciplinary procedure is necessary are deleted within 2 months from the end of the verification/ investigation phase.
- reports leading to a litigation/disciplinary procedure are deleted once applicable legal statute of limitation periods have expired.

#### **11. Are your data safe and secure?**

Oerlikon has taken organizational and technical measures to protect the security and confidentiality of your personal data:

- A data processing agreement has been signed with our supplier People Intouch who is in charge of receiving and storing reports made through the Speak up phone line or platform;
- Limited and protected access rights to reports: at Oerlikon, only the Head of Internal Audit and Head of Compliance can access the reports made through the Speak Up App, phone line or online platform. More generally the competent person to whom you have reported (based on the Reporting policies) is required to keep your report confidential;
- The Reporting Policies poses as an obligation for all Oerlikon entities to protect the privacy, rights and safety of the Reporting person, witnesses and the accused person and prohibit any retaliation measure when a report is made in good faith.
- The Reporting person is provided with a case number when she reports through the phone line or online platform. This case number enables her to follow up the case. Nobody else has this Case number which means that nobody else can follow up on her report. When the Reporting person reports through the Speak Up app she must create a PIN, once she downloads it, scan the QR code, then insert the organisation code shared by Oerlikon to be able to leave a message in Speak- Up



## **12. Changes to the Privacy Notice**

Any change to the Reporting Policy and related Privacy Notice will be duly communicated in our intranet, online Reporting platform, to our works councils (or any equivalent body) where legally required, our employees and business contacts. In any case, the aim of our changes will never be to jeopardize the rights and privacy of the Reporting person, accused person, witnesses or any third party mentioned in any report or exempt us from our legal obligations.