



PROCEDURE FOR MANAGING REPORTS SENT TO THE "SPEAK UP" CHANNEL

DATE OF ISSUE: October 2025

1. PREMISE.....	1
2. SCOPE OF APPLICATION: WHO CAN REPORT AND TO WHOM THE PROCEDURE IS ADDRESSED.....	1
3. RECIPIENTS OF REPORTS.....	2
4. REPORTS.....	2
5. PROTECTION OF THE REPORTER.....	3
6. DOCUMENT ARCHIVING.....	4

1. PREMISE

OVS has adopted an additional reporting channel, in addition to the Whistleblowing channel, which allows employees, suppliers, customers, and any other subject in a relationship with OVS S.p.A. to submit written reports relating to violations of company conduct rules or policies or procedures, such as abuses, harassment and discrimination in the workplace, non-compliance with the code of conduct for suppliers, violations of the Equity, Diversity and Inclusion policy.

The policies described above are available on the corporate website and on WELLO (company intranet) in the section OVS SpA > Policies and Procedures. This procedure has been drawn up to describe the methods, recipients and timing for managing reports sent through the "OVS SPEAK UP" channel, which can be sent in writing through the reporting channel on the corporate website and on the company intranet.

2. SCOPE OF APPLICATION: WHO CAN REPORT AND TO WHOM THE PROCEDURE IS ADDRESSED

This procedure applies to all subjects of the Company or connected to it, both senior and subordinate.

2.1 OBJECT OF REPORTS

Reports may concern information relating to:

- Cases of harassment and discrimination in the workplace.
- Non-compliance with company policies on environment and human rights (Climate and Energy Policy, Environment and Territory Policy, Human Rights Policy, Diversity, Equity and Inclusion Policy, Due Diligence Policy, Code of Conduct).

2.2 CONTENT OF REPORTS AND RESPONSIBILITY OF THE REPORTER

Reports must be made in good faith and must be based on precise factual elements of which the Reporter has direct knowledge (seen directly or 'suffered').

The Reporter must provide all useful elements to allow the competent subjects to proceed with the necessary and appropriate verifications and investigations to ascertain the foundation of

the facts subject to the report.

2.3 WHAT A REPORT MUST CONTAIN

The report in particular must contain the following elements:

1. a clear and complete description of the facts subject to the report;
2. the circumstances of time and place;
3. any other relevant information.

3. RECIPIENTS OF REPORTS

The recipient of the report is an internal company committee, composed of Human Resources and Organization, Corporate Sustainability, Legal Affairs and Internal Audit.

4. REPORTS

Methods of sending reports

Reports can be made in writing using a dedicated IT platform accessible through the website www.ovscorporate.it in the Governance section.

Management of the reporting channel

Within the scope of managing the reporting channel, the committee receiving the Reports carries out the following activities:

- provides feedback on the receipt and handling of the report, requesting integration if the details provided are not sufficient;
- carries out investigations, also where deemed necessary with the support of OVS offices, regarding the reports received (specific analyses aimed at ascertaining the veracity of the facts or circumstances subject to the report, while protecting the confidentiality of the reporter's identity).

The verification actions on the foundation of the circumstances represented in the reports will be carried out in compliance with the principles of impartiality and confidentiality, carrying out every activity deemed appropriate and involving the competent company functions.

At the conclusion of the preliminary investigation phase, the Committee receiving the Reports makes consequent decisions, archiving, where appropriate, the report if it turns out to be an irrelevant or insufficiently proven report.

5. PROTECTION OF THE REPORTER

Obligations of confidentiality on the identity of the Reporter

With the exception of cases in which liability for slander and defamation can be configured

pursuant to the provisions of the criminal code or article 2043 of the civil code and cases in which anonymity is not enforceable by law (for example: criminal, tax or administrative investigations, inspections by control bodies), the identity of the Reporter is protected in every context subsequent to the report.

Therefore, without prejudice to the exceptions mentioned above, the identity of the Reporter cannot be revealed without their express consent and all those who receive or are involved in the management of the report are required to protect the confidentiality of this information.

With regard to, in particular, the scope of disciplinary proceedings, the identity of the Reporter can be revealed to the disciplinary authority and to the accused only in cases where:

- there is the express consent of the Reporter;
- the disciplinary charge is founded, in whole or in part, on the report and the knowledge of the Reporter's identity is absolutely indispensable for the defense of the accused, provided that this circumstance is deduced and proven by the latter during the hearing or by presenting defensive briefs.

In the latter case, the Reporter is notified, by written communication, of the reasons for the disclosure of confidential data, as well as of the internal reporting procedures when the disclosure of the Reporter's identity and information is indispensable for the defense of the person involved.

Processing of personal data

All processing of personal data must be carried out in accordance with the GDPR and Legislative Decree no. 196/2003 as amended by Legislative Decree 101/2018 (Privacy Code).

Data that are manifestly not useful for the processing of a specific report must not be collected or, if accidentally collected, must be deleted immediately.

The processing of personal data is carried out by the Data Controller, providing suitable information to the reporting persons and the persons involved pursuant to articles 13 and 14 of the GDPR.

Pursuant to art. 2 undecies co. 1 lett. f), of the Privacy Code, the rights referred to in articles 15 to 22 of the GDPR may be limited or cannot be exercised by requesting the Data Controller if their exercise could cause actual and concrete prejudice to the confidentiality of the identity of the employee who reports, pursuant to Law 179/2017, the unlawful act of which they became aware by reason of their office.

Prohibition of discrimination against the Reporter

The Company does not tolerate threats or retaliation of any kind against the Reporter or anyone who has collaborated in verifying the foundation of the report.

It is understood that all disciplinary initiatives eventually undertaken for retaliatory purposes will be considered null and void.

6. DOCUMENT ARCHIVING

The Committee receiving the Reports is required to document, by keeping electronic and/or paper documents, the reports received, in order to ensure the complete traceability of the interventions undertaken for the fulfillment of its institutional functions.

Electronic documents are stored in an IT archive MOD 06.01 "Register of non-conformities and corrective actions" managed and updated by the Committee receiving the Reports.

In the case of reports produced in evident bad faith, the committee receiving the reports reserves the right to archive them by deleting the names and elements that could allow the identification of the reported subjects.

The data thus collected and archived will be kept by the committee receiving the reports for a period of 5(five) years.