



WHISTLEBLOWING HANDBOOK

Rev 1.0, November 30, 2023

© Copyright OverIT

The information contained within this document is property of OverIT. Any permitted use is based on the level of restriction specified in the header. The restriction level is assigned according to the Data Classification Policy. Certain prospective user entities, identified by OverIT as "Recipient(s)", may have access to this document subject to OverIT's explicit authorization. If you are not one of these intended Recipients, please close and discard this document.

Document approval information

Department	
Responsibility:	Legal & Sustainability

Revision History

Revision	Date	Summary of amendments
1.0	27 June 2023	First drafting of the Whistleblowing Handbook

Index

1. Introduction	4
1.1. Who are the reporting persons (Whistleblowers)?	4
1.2. What can be reported?	4
1.3. Who are the recipients of the reports?	5
1.4. What are the safeguards for the reporting persons?	6
1.4.1. Protection of confidentiality	6
1.4.2. Prohibition of discrimination	6
2. How can I submit a report?	6
3. How to monitor a report?	12
4. Timing	15

1. Introduction

OverIT S.p.A. (hereinafter referred to as "OverIT" or "Company") and the companies under the management and control of OverIT (hereinafter referred to as the "OverIT Group") operate with loyalty, transparency, honesty and fairness, in compliance with applicable laws, regulations and standards.

In order to comply with the provisions of Legislative Decree No. 24, March 10th, 2023 (implementing Directive (EU) 2019/1937 on Whistleblowing), OverIT Group has adopted a reporting management process and has set up a confidential and multilingual IT platform for the reporting of alleged breaches (so-called Whistleblowing Platform) which can ensure the confidentiality and anonymity of the reporting person, in accordance with the relevant European and national legislation (so-called Whistleblower).

1.1. Who are the reporting persons (Whistleblowers)?

A Whistleblower is a natural person who makes a report on breach information acquired within his or her work-related context with OverIT Group companies.

In particular, the following subjects may assume the role of Whistleblower:

- employees;
- self-employed individuals (e.g., consultants, suppliers of goods and services, agents, contractors/sub-contractors and business partners);
- paid or unpaid volunteers and trainees;
- shareholders and persons with administrative, management, control, supervisory or representative (also de facto) functions.

The subjects above may also make a report when the relationship with OverIT Group companies is not formally in place, for instance:

- when the employment relationship has not yet started (selection or recruiting phase);
- during the trial period;
- following the dissolution and termination of the relationship.

1.2. What can be reported?

Breaches of national or Union law that harm the public interest or the integrity of public administration or private entity, which the reporting person became aware in the work-related context, are subject to reporting.

In particular:

- breaches of Union law (e.g. public procurement; financial services, products, and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; public health; consumer protection; privacy and data protection; network and information system security);
- administrative, accounting, civil or criminal offences;

- illegal conduct relevant to Legislative Decree No. 231, June 8th, 2001, attempted breaches and/or breaches (including alleged breaches) of OverIT's Organization, Management and Control Framework;
- attempted breaches and/or breaches (also alleged breaches) of OverIT's Code of Ethics;
- attempted breaches and/or alleged or proven breaches of Company's procedures or internal regulatory system;
- attempted breaches and/or ESG-related breaches, namely relating to the Company's social and environmental responsibility activities.

The report may also relate to:

- information regarding conduct aimed at concealing the above breaches;
- unlawful activities – not yet performed – the reporting person reasonably believes may occur in the presence of concrete, precise and consistent elements;
- the founded suspicions of breaches.

Legislative Decree No. 24/2023 does not apply to complaints, claims or requests related to a personal interest of the reporting person, pertaining exclusively to his/her individual employment relationship, even with reference to figures hierarchically superordinate figures to him/her.

1.3. Who are the recipients of the reports?

Reports are properly assessed, verified, and managed by the Supervisory Board, in the capacity of reporting manager, by sending them to the following e-mail address: omc_supervisorybody@overit.it

Where the reports concern the Supervisory Board or its individual members, the reporting persons may transmit the reports directly to the Board of Directors through the following channel: omc_boardofdirectors@overit.it

The reporting person may use the external reporting channel made available by the Italian Anticorruption Authority (ANAC) where:

- he/she has not received response to the report submitted;
- he/she has founded reason to believe – based on attached factual circumstances and effectively acquired information – that, if he/she submitted an internal report, it would not be effectively followed up or there may be a risk of retaliation;
- he/she has founded reason to believe that the breach may present an imminent or obvious danger to the public interest.

Moreover, other whistleblowing channels to report notices related to social responsibility and worklabour conditions, as for international standard SA8000, are the following:

- DVN Certification Entity, writing to: feedback.italia@dnv.com;
- Through the Body of Accreditation SA8000 (SAAS – Social Accountability Accreditation Services - 15 West 44th Street, 6th Floor - New York - NY 10036), writing to: saas@saasaccreditation.org.

1.4. What are the safeguards for the reporting persons?

1.4.1. Protection of confidentiality

- The identity of the reporting person shall not be disclosed to persons other than those charged with receiving and following up reports.
- The identity of the Whistleblower and any other information from which his/her identity may be inferred, directly or indirectly, shall not be disclosed – without the express consent of the whistleblower himself/herself – to persons other than those charged with receiving and following up reports.
- The confidentiality of the identity of the persons involved and mentioned in the report shall be ensured until the conclusion of the proceedings, subject to the same safeguards as for the reporting person.

1.4.2. Prohibition of discrimination


- Pursuant to Article 17 of Legislative Decree No. 24/2023, OverIT ensures the protection of the reporting person from acts of retaliation or discrimination ("*any direct or indirect act or omission, even attempted or threatened, prompted by reporting, reporting to judicial or accounting authorities or public disclosure, which causes or may cause unjustified detriment (directly or indirectly) to the reporting person or the person who filed the complaint*").
- Direct or indirect acts of retaliation against the reporting person for reasons related, directly or indirectly, to the report made shall be prohibited.

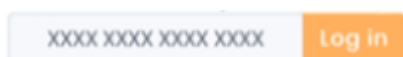
2. How can I submit a report?

Reports can be submitted via the "Whistleblowing" platform accessible at: <https://overit.whistleblowing.it/>

In order to send a report, the user (reporting person) must access the main screen of the "Whistleblowing" platform (see Image 1), which is available in both Italian and English. It is possible to use the platform with any device, fixed or mobile (e.g. PC; Tablet; cell phone).

From the main page, the reporting person can:

- enter a new report by clicking on the button 
- retrieve a previously submitted report by entering the 16-digit report code (key code)




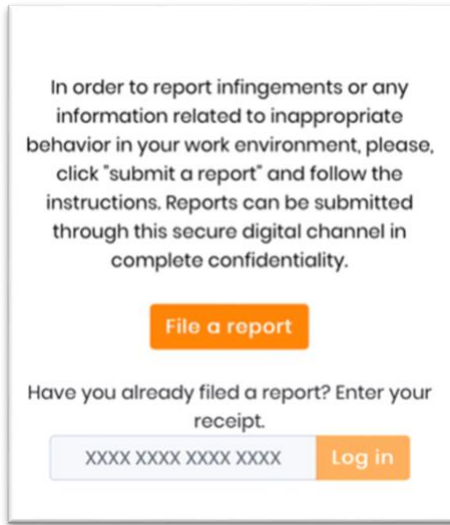
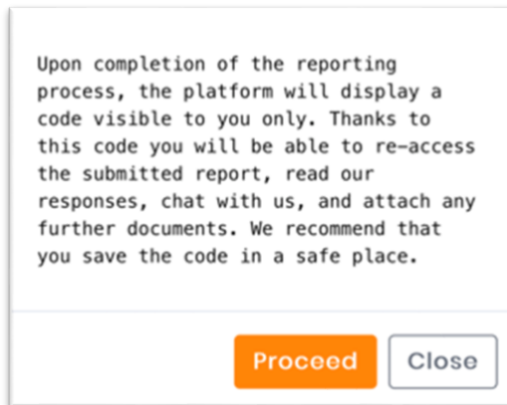
XXXX XXXX XXXX XXXX 

Image 1 - Homepage – Whistleblowing



By choosing to submit a new report, the user will see an alert (see Image 2) regarding the need to store, at the end of the process, the report code in order to monitor, integrate and manage the reports already submitted.

Image 2 – Initial alert



By moving forward, the reporting person will see the following screen where he/she should enter the initial information about the report. In particular, the reporting process consists of 4 sections:

1. preliminary information;
2. fill out your report;
3. general information;
4. final step.

In order to move forward through the different sections and properly complete the entire reporting process, the reporting person shall complete all required fields (marked with the symbol *).

In the "**Preliminary Information**" section, the reporting person shall indicate to which organizational structure the report relates (see Image 3) by alternately selecting OverIT S.p.A., OverIT International Inc. or OverIT U.K. LTD.

Image 3 – Preliminary Information

On the same screen, the reporting person shall indicate the type of relationship he/she has with the company involved, by selecting between employee, collaborator, supplier, business partner or other (e.g. paid or unpaid volunteers and trainees, shareholders, etc.). The interfaces for entering reports are identical for any selected company; therefore, the functionality of an individual organizational structure will be described below.

Once the required fields are populated (marked with the symbol *) with the data requested, the reporting person should click on the button [Next](#) to move forward or on the button [Previous](#) to return to the previous screen.

In the "**Fill Out Your Report**" section, the reporting person shall provide any information **relating to possible breaches or conducts not consistent with the rules adopted by the Company. The reporting person shall submit detailed reports of alleged misconduct based on precise and consistent factual elements.**

To this end, the report shall contain, where possible, the following elements:

- the type(s) of offence(s) intended to be reported (see Image 4);
- the level of involvement of the reporting person;
- a description as clear as possible of the facts reported;
- the circumstances of time and place in which the reported facts occurred, where known;
- the indication of any other person who may report on the facts reported;
- any other information that may provide useful support in establishing and verifying the existence of the facts reported.


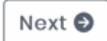

The report may be integrated – attaching any documentation or evidence supporting the alleged wrongdoing – by using the button 

Image 4 – Fill Out Your Report



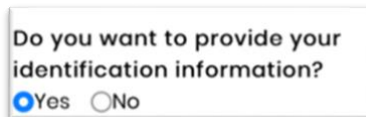
What type of non-compliance are you willing to report? *
You may report more than one infringement but we recommend the highest accuracy so as to support fact-finding.

- Violations of the organizational model 231/2001
- Anti-corruption and bribery policy
- Code of Ethics
- Staff Handbook
- Others

Once the required fields are populated (marked with the symbol *) with the data requested, the reporting person should click on the button  to move forward or on the button  to return to the previous screen.

By choosing to move forward, the reporting person will see the following screen called "**General Information**". Within this screen, the reporting person shall make the choice of providing his/her identification data or transmitting the report anonymously (see Image 5).

Image 5 – Anonymous Report



Do you want to provide your identification information?
 Yes No

If the reporting person chooses not to provide his/her identity, the interactions between the reporting manager and the reporting person will take place through the *Whistleblowing* platform. In particular, the reporting person will be able – through the platform – to monitor updates on investigations and provide, upon request, any insights or clarifications regarding the report submitted.

Conversely, if the reporting person chooses to provide his/her identification data, he/she shall enter his/her name in the appropriate fields and selects the contact method preferred (see Image 6).

Image 6 – Confidential Report

Do you want to provide your identification information?
 Yes No

First name *

Last name *

Alternative contact method *

Image 7 – Contact Method

Do you want to provide your identification information?
 Yes No

First name *

Last name *

Alternative contact method *

- I prefer to be contacted via this platform only
- Email address
- Phone number
- Other

Once the required fields are populated (marked with the symbol *) with the data requested, the reporting person should click on the button **Next** to move forward or **Previous** on the button to return to the previous screen.

On the last screen called "**Final Step**," the reporting person is asked to read carefully the "Privacy Notice" and the alert regarding the need to keep the personal *key code* generated by the system at the end of the reporting process. For both notices, the reporting person is required to check the relevant boxes for acknowledgement of the notices (see Image 8).

Image 8 – Final Step

Privacy Policy *

Please, download the privacy policy at this [link](#)

Please tick the acknowledgement check box

REMEMBER TO KEEP YOUR PERSONAL KEY CODE IN A SAFE PLACE *

Lacking the provision of alternative contact modalities, this platform shall be the sole communication channel with you, along with the dedicated key code, which is generated by the system and will appear on the web page after submitting the report. Please, keep the key code in a safe place and do not disclose it to third parties, as you will need it to access the platform, read our answers, and chat with us in a secure, confidential, or anonymous way.

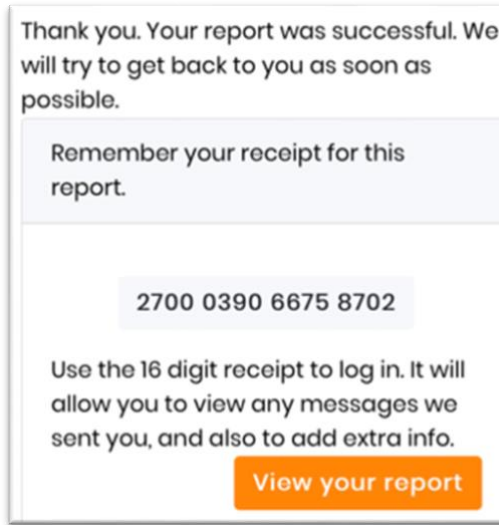
Please tick the acknowledgement check box

In order to return to the previous screens, the reporting person should click on the button and to move forward and submit the report, the reporting person should click on the button



Once the report is transmitted, the system generates automatically the *key code* identifying the report (see Image 9).

Image 9 – Key code (example)



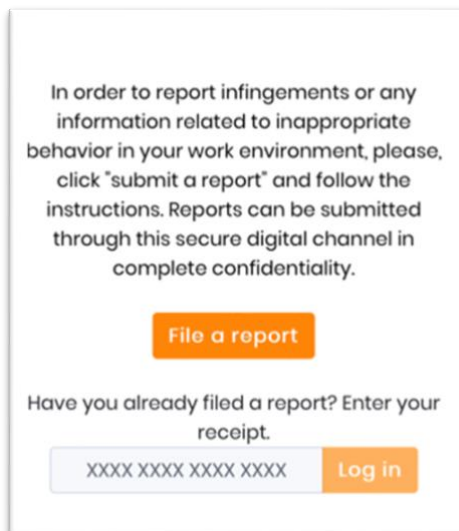
The *Key code* provides for the possibility to monitor the progress of the report, integrate the report transmitted with any additional documentation and information and interact – via private messages – with the Supervisory Board, in the capacity of reporting manager, while maintaining the utmost confidentiality.


By clicking on the [View your report](#) button the reporting person accesses the page with the complete data of the report just made.

3. How to monitor a report?

To monitor the progress of the report, the reporting person shall enter the *Key code* in the appropriate field in the lower area of the main page of the system (see Image 10).

Image 10 – Homepage – Whistleblowing



Once the code is entered, the reporting person accesses – by clicking on the button  – the page of the report (see Image 11) where he/she can find updated information relating to:

- the status of progress of the report (e.g. open; closed);
- the data of the report;
- the identification data of the reporting person, where provided.

Image 11 – Status of progress of the report (example)

 Date	 Last update	 Expiration date	 Reminder date
14-07-2023 10:06	14-07-2023 10:15	15-07-2028	Closed


Within the same page, the reporting person can find two areas called “Attachments” e “Comments” respectively, where he/she can integrate, via file and textual content, the report transmitted. In particular, by entering the comment in the appropriate field (see Image 12) and by clicking on the button , the reporting person may send private messages to the reporting manager (see Image 13).

Image 12 – Communications with the reporting manager (example)

Comments ^

0/4096




Image 13 – Communications with the reporting manager – Anonymous mode (example)

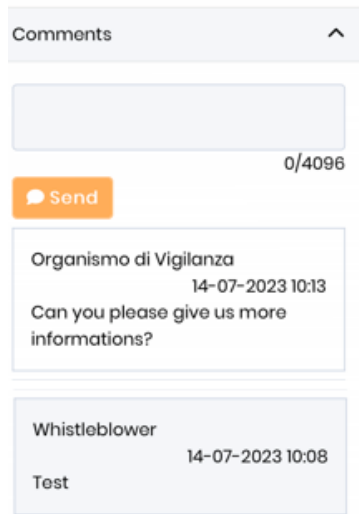
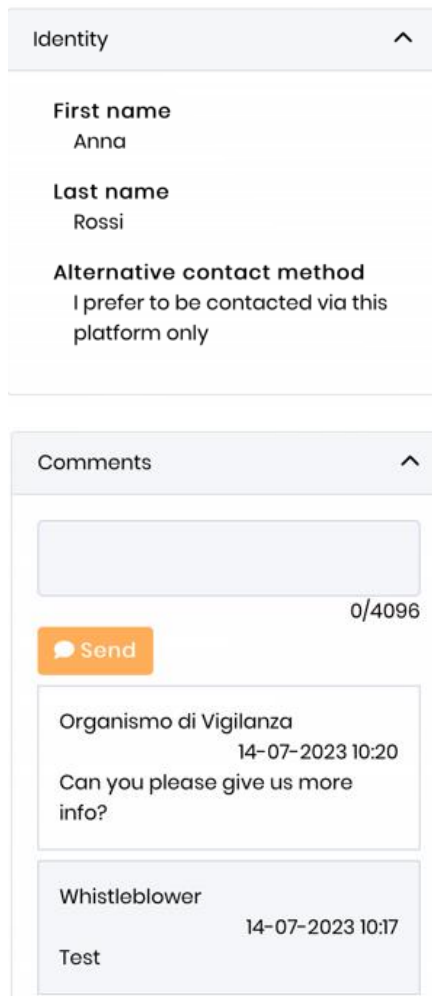


Image 13 – Communications with the reporting manager – Confidential mode (example)



The reporting person is recommended to access periodically the Whistleblowing Portal to check for any requests for clarification related to the report submitted.

4. Timing

The Supervisory Board, in the capacity of reporting manager, shall:

- provide feedback to the reporting person on the taking charge of the report **within 7 days**;
- provide formal feedback to the reporting person **within 3 months** of the submission by the reporting person.

Once the investigation is closed, the reporting person still has visibility of the report submitted, but he/she can no longer make further changes to it (e.g. attach additional documents; send comments to the reporting manager; etc.). The Key code is valid until the expiration of the report (i.e. 5 years).