

WHISTLEBLOWING INSTRUCTION

Netsens Srl

Version 1

Revision	Publication date	Reason for revision
1	07/01/2026	First Release



INDEX

1.	Purpose.....	4
2.	Normative context.....	4
3.	Introduction to whistleblowing.....	4
4.	Departments and stakeholders.....	5
5.	Ways and timescales for handling alerts: Internal channel.....	6
6.	ANAC channel.....	6
7.	Other external channels.....	6
8.	Protection and support measures.....	6
9.	Retaliation and Reporting.....	7
10.	Procedures and other related documents.....	7
11.	Description of the Procedure.....	7
12.	Handling of reports and investigation by the Supervisory Board.....	8
13.	The protection of the reporter.....	8
14.	Operational modes of transmission reporting.....	9

1. Purpose

The purpose of this document is to define the operating procedures for the management of reports and any ensuing investigations, with regard to the offences envisaged by Legislative Decree no. 24/2023 and conduct relevant pursuant to the Code of Ethics, based on objective, precise and concordant findings, or violations of Netsens Srl's Organisation and Management Model, as already set out in Protocol 231 "RELATIONS WITH PUBLIC ADMINISTRATIONS, ANTI-CORRUPTION RULES AND "WHISTLEBLOWING" PROCEDURE".

2. Normative context

The Legislature passed Law No. 179 of 30 November 2017, containing "Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship" (so-called "Whistleblowing Law")

The Decree-Law No. 24/2023 transposing Directive (EU) 2019/1937 and repealing certain provisions of Legislative Decree No. 231/2001 and Law No. 179/2017 was issued (on 9 March 2023, and published in the Official Gazette on 15 March 2023).

This procedure reflects the legislation in force and applies the ANAC guidelines approved by resolution 311 of 12/7/2023 and the guidelines issued by Confindustria in October 2023.

These provisions apply to all private entities that have employed at least 50 workers in the last year, and to entities that adopt organisation and management models (Legislative Decree 231/2001)

3. Introduction to whistleblowing

Whistleblowing' is a report made by a person inside or outside the company who detects a violation of the whistleblower's work environment:

- Torts
- Administrative offences
- Offences under Legislative Decree No. 231/2001 and violations of the operating protocols of the Organisation and Management Model and/or the Code of Ethics drawn up and disseminated pursuant to Legislative Decree No. 231/01.
- Offences related to the violation of EU law;
- acts or omissions detrimental to the EU's financial interests;
- acts or omissions relating to the internal market, free movement of goods, persons, services and capital (including matters of competition and State aid, taxation to obtain a tax advantage);
- acts or conduct that frustrate the object and purpose of laws and regulations as well as those protecting the EU's financial interests and regulating the internal market;
- Conduct aimed at concealing the above violations.

Netsens Srl, in application of the Code of Ethics, has implemented reporting systems to allow persons entitled to report acts or facts that may constitute conduct that is incompatible with the Organisation, Management and Control Model in force pursuant to Legislative Decree 231/01 or with the other types of violations identified above.

By way of example only and certainly not exhaustively, therefore, acts or facts concerning conduct or behaviour such as

- improper use of the powers and delegations granted;
- misrepresentation, falsification/obstruction of financial, accounting/tax records and other serious administrative or tax violations;
- payments and disbursements to unauthorised persons and/or in violation of the internal

- authorisation process, including for the purpose of internal fraud, theft and embezzlement;
- false signing of contractual documents or dispositive forms;
 - activities carried out in a situation of conflict of interest;
 - violations of corporate and financial transparency provisions;
 - unlawful access to information systems and/or unlawful data processing, including through the use of credentials of other persons;
 - violations of corporate protocols 231/01;
 - violation of rules and procedures for the prevention of risks in the field of food safety, occupational safety, environmental protection regulations and data privacy.

It is understood that the reports must have fundamental and circumspect characteristics and must therefore be clear in the circumstances of time and place, in the description of the fact and in generalities or other elements that allow the identification of the person to whom the fact is attributed.

The following are excluded from the scope of the procedure:

- reports on situations of a personal nature concerning claims or grievances relating to relations with hierarchical superiors or colleagues, as well as relating to the performance of one's work;
- reports based on mere suspicions, rumours, unreliable indiscretions (ex. rumours)
- reports that are unfounded or already totally in the public domain

Anonymous reports are taken into account and treated in the same way as ordinary reports.

4. Departments and stakeholders

The subjective scope of application of this discipline has become very broad with Decree 24/2023 and thus extends no longer only to those who qualify as employees but to the outside world.

The persons involved in the activities under this procedure and protected in the event of a report are:

- Candidates (if information on violations was acquired during the selection process or in other pre-contractual steps)
- All employees, including probationary employees, who may report violations of the Netsens Srl Organisation and Management Model, of which they have become aware by reason of the functions/assignments performed;
- Former employees (if information on violations was acquired in the course of employment)
- Self-employed workers, collaborators, trainees and volunteers (including unpaid workers or those with agency or commercial collaboration contracts) working for private sector entities
- Managing Director, shareholders and persons with administrative, management, control, supervisory or representative functions (also de facto)
- Suppliers of goods and services and consultants

Moreover, persons other than those who report but who may be subject to retaliation because of their role in the reporting process also enjoy the same protections:

- The Facilitator: one who assists the reporter and belongs to the same work context
- Staff in the same work environment with a stable emotional link to the reporter
- Work colleagues of the reporter
- Entities owned by the reporter
- Entities to which the reporter makes public disclosure
- Entities operating in the same context as the reporter

5. Ways and timescales for handling alerts

5.1 Internal Channel

The channels through which the decree gives the possibility to submit reports are different.

- Internal channels of private entities
- External channel at ANAC
- Public Disclosure
- Complaint to the judicial authority.

The internal channel described below has been defined within the MOG 231 and guarantees the levels of confidentiality and modalities required by law.

Reports can always be made in written and oral form.

The persons who receive reports, which may be either internal or external, must be defined. Netsens Srl, having established the OMC 231, entrusts the management of reports to its Supervisory Board and internally to the Administrative Department.

The supervisory body issues the reporting person with an acknowledgement of receipt of the report within 7 days from the date of receipt.

The proceedings initiated following receipt of the report must be concluded, with acknowledgement, within 3 months from the date of the acknowledgement of receipt (or, failing that, 7 days from the submission of the report).

The terms of access and this information notice are published on the company's corporate website and thus available to all stakeholders.

If persons outside those listed above receive reports that are clearly of the whistleblowing type, they are obliged to forward such reports to the relevant persons within 7 days of receipt.

The establishment and publication of this procedure and reporting methods are subject to a formal act in accordance with the OMC 231.

The characteristics of confidentiality and the way in which data is processed are published in the privacy policy.

5.2 ANAC channel

The ANAC (National Anti-Corruption Authority) has set up an electronic and a telephone channel for reporting according to the regulations, as one of the possible ways of reporting.

The online platform can be reached at: <https://www.anticorruzione.it/-/whistleblowing>

The telephone channel can be reached at: +39 06 36723368

Both modes reflect the characteristics of confidentiality required by law.

5.3 Other external channels

Please also note that two other external channels for reporting whistleblowing are also available, which can only be used if the previous two channels (internal and ANAC) were unsuccessful:

- PUBLIC DISCLOSURE: through the press and other media
- The complaint to the judicial AUTHORITY

6. Protection and support measures

The legislation provides a set of protections for the reporter:

- Protection of the confidentiality of the reporter and all persons involved
- Protection from retaliation
- Limitation of liability with respect to detection

7. Retaliation and Reporting

Retaliation is any act, conduct or omission, even if only attempted or threatened, that causes or is likely to cause unfair harm to the whistleblower or persons involved with the whistleblower.

Alleged retaliation must be reported exclusively to ANAC through the channels provided by the body.

The finding of retaliation provides for administrative sanctions as well as the nullity of the effects of the retaliation.

8. Procedures and other related documents

- Organisation, Management and Control Model pursuant to Legislative Decree No. 231 of 8 June 2001;
- Code of Ethics Netsens Srl;
- 231/01 company protocols and internal procedures
- Whistleblowing privacy policy

9. Description of the procedure

In compliance with D.gls. 24/2023 and its Organisational, Management and Control Model pursuant to Legislative Decree 231/01, the procedures for transmitting to the Supervisory Board reports concerning conduct that may constitute the possible commission of offences.

In order to facilitate reporting, the following channels have been defined:

- through the **integrityline.com** web application, as the primary reporting channel suitable for guaranteeing, by computerised means, the confidentiality of the reporter's identity, in compliance with the legislation (hereinafter, the 'Software'), it is explained how the individual employee can access the Software; this mode also has the possibility of leaving voice messages with a disguised voice.
- by means of a sealed envelope sent by Netsens Srl with the name "CONFIDENTIAL PERSONAL" and addressed to the Chairman of the Supervisory Board, which the function in charge of sorting mail must immediately and confidentially forward to the professional address of the same. The envelope must contain two sealed envelopes, the first with the identification data of the reporting person together with a photocopy of the identification document; the second with the report, so as to separate the identification data of the reporting person from the report.

The procedure normally requires the identification of the whistleblower, who is protected in the forms described below: however, Netsens Srl will also take anonymous reports into consideration if they are adequately circumstantiated in terms of places, times and methods of execution, and are such as to reveal specific contexts (e.g.: documentary evidence, indication of names or particular qualifications, mention of specific offices, proceedings or particular events, etc.).

The report - even the non-anonymous one - must be circumstantial and as complete and exhaustive as possible.

The whistleblower is required to provide all the available and useful elements to enable the competent persons to carry out the due and appropriate checks and verifications to confirm the validity of the reported facts.

For a report to be substantiated, these requirements do not necessarily have to be present at the same time as the report, in view of the fact that the reporter may not be in full possession of all the information requested.

Through the IT channel and thus through the software, the reporter will be guided through each stage of the reporting process and will be asked, in order to better substantiate the report, to fill in a series of fields that must be completed in accordance with the requirements.

It is essential that the elements indicated are known directly to the reporter and not reported or referred to indirectly by others.

10. Handling of reports and investigation by the Supervisory Board

Once the report has been received according to the channels envisaged in this procedure, the Supervisory Body will start the investigation as defined in the protocol "RELATIONS WITH PUBLIC ADMINISTRATIONS, ANTICORRUPTION RULES AND "WHISTLEBLOWING" PROCEDURE".

11. Protecting the reporter

The entire process must in any case guarantee the confidentiality of the identity of the whistleblower from the moment the report is received and at every stage thereafter, unless ordered by the judicial authorities.

To this end, Netsens Srl protects all whistleblowers by providing in its protocol "RELATIONS WITH PUBLIC ADMINISTRATION, ANTICORRUPTION RULES AND "WHISTLEBLOWING" PROCEDURE":

The protection of the confidentiality of the reporter:

- The identity of the reporting person may not be disclosed to persons other than those entrusted with the task of managing the reporting channel or with the task of following up the reports, unless:
 - the reporting person has not given his or her express consent
 - knowledge of the identity of the whistleblower is not indispensable for the defence of the accused in disciplinary proceedings following a charge based, in whole or in part, on the report submitted (but the express consent of the whistleblower is always required to use the report for disciplinary purposes)
 - knowledge of the identity of the whistleblower is not indispensable for the defence of the accused or the person involved in the management proceedings

The prohibition of discrimination against whistleblowers.

Legislative Decree No. 24/2023 provides for a general prohibition of retaliation against persons who make reports, public disclosures or complaints. The protection also extends to the facilitators and colleagues of whistleblowers.

They are considered retaliatory acts, for instance:

- dismissal, suspension or equivalent measures
- downgrading or non-promotion
- change of duties, change of place of work, reduction of salary,
- modification of working hours
- suspension of training or any restriction of access to it
- negative merit notes or negative references
- the adoption of disciplinary measures or other sanction
- coercion, intimidation, harassment or ostracism
- discrimination or otherwise unfavourable treatment
- non-renewal or early termination of a fixed-term employment contract
- reputational damage economic or financial damage

12. Operational modes of transmission reporting

1. Access the link <https://ibfservizi.integrityline.com/>,

Sistema di segnalazione

Nel sistema di segnalazione è possibile segnalare in modo rapido e semplice preoccupazioni in merito alla cattiva condotta, effettiva o sospetta, che può avere effetti negativi sulla nostra azienda o sul benessere delle persone.

Il sistema di segnalazione non può essere usato per muovere accuse fallaci contro terzi e, in generale, non possono essere segnalate informazioni deliberatamente inesatte.

Ti invitiamo a fornirci il tuo nome nella segnalazione. Che tu lo faccia o no, ti preghiamo comunque di aprire una Inbox, la casella di posta sicura. In questo modo, sarà più semplice e sicuro comunicare tra noi.

Tutte le segnalazioni sono strettamente riservate. Puoi trovare maggiori informazioni al riguardo nella sezione menu "Informativa sulla privacy", qui sopra.

Le segnalazioni relative a potenziali comportamenti illeciti negli Stati membri dell'Unione Europea o identificate da segnalanti all'interno dell'Unione Europea possono essere segnalate anche ad autorità esterne. Puoi trovare una panoramica [qui](#).



2. After reading the instructions, click on 'Send Report'.





- filling in the form by entering the requested data (please do not use the company e-mail account, as required by the Privacy Guarantor)

Invia una segnalazione

Qual è il tuo sospetto? ***Obbligatorio**

Lavori nell'organizzazione? Scegli un'opzione

In quale azienda ha avuto luogo l'incidente?

Indicare il nome del dipartimento interessato:

Chi è coinvolto nell'incidente?

In quale Paese si è verificato l'incidente?

In quale città si è verificato l'incidente?

Informazioni di contatto

Puoi scegliere di inviare la segnalazione in forma anonima, ma ti invitiamo a fornire il tuo nome e i dati di contatto nei campi sottostanti.

Desidero rimanere anonimo

Nome

Numero di telefono

E-mail

Inbox sicura

Si prega di aprire una casella di posta elettronica sicura creando una propria password, anche se si sono già inseriti i propri dati di contatto. In questo modo, sarà più semplice e sicuro comunicare la news.

Utilizza la Inbox - casella postale se desideri inviare ulteriori informazioni o rispondere a potenziali domande.

Quando chi la Inbox, ti sarà assegnato un numero della segnalazione e soglierai a una password. Che il numero della segnalazione e la password per accedere alla Inbox e vedere se hai ricevuto domande. Se lo desideri, tutte le nostre comunicazioni saranno anonime.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una segnalazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

Inserisci la tua password

La password deve:

- Avere una lunghezza minima di 8 caratteri.
- Essere composta almeno da una lettera minuscola e una maiuscola.
- Contenerne almeno un numero.

Password

Reinserisci nuovamente la password

Ho letto e accetto l'informazione sulla privacy e accetto.

- Please note that, if you wish, you may send your report anonymously, if it is adequately circumstantiated as to the place, time and manner of execution, and made in such a way as to reveal specific contexts (e.g. documentary evidence, indication of particular names or qualifications, mention of specific offices, proceedings or particular events, etc.).

Informazioni di contatto

Puoi scegliere di inviare la segnalazione in forma anonima, ma ti invitiamo a fornire il tuo nome e i dati di contatto nei campi sottostanti.

Desidero rimanere anonima/o

Nome

Numero di telefono

E-mail

5. It is possible to insert attachments such as files or photos, or to record voice messages (where the voice will be disguised) using the controls at the top right of the page

Inviare una segnalazione



6. Carefully read the instructions on the InboxSecure

Inbox sicura

Si prega di aprire una casella di posta elettronica sicura creando una propria password, anche se si sono già inseriti i propri dati di contatto. In questo modo, sarà più semplice e sicuro comunicare tra noi.

Utilizza la Inbox - casella postale se desideri inviare ulteriori informazioni o rispondere a potenziali domande.

Quando crei la Inbox, ti sarà assegnato un numero della segnalazione e sceglierai una password. Usa il numero della segnalazione e la password per accedere alla Inbox e vedere se hai ricevuto domande. Se lo desideri, tutte le nostre comunicazioni saranno anonime.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una registrazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

7. Enter the password to be used later, together with the report number to access the secure inbox, then make sure to keep the password entered securely.

Inserisci la tua password

La password deve:

- Avere una lunghezza minima di 8 caratteri.
- Deve contenere almeno una lettera minuscola e una maiuscola.
- Contenere almeno un numero.

Ho letto e capito l'Informativa sulla privacy e accetto.

8. Accept the privacy policy that is always available on the home page of the site.
9. Proceed to send the report with the 'Send' button
10. The software will display confirmation that the report has been sent and will show the report number, which you will need to access your secure inbox

Conferma

Grazie. Abbiamo ricevuto la tua segnalazione. Inizieremo a trattare il tuo caso il più presto possibile.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una registrazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

Importante:

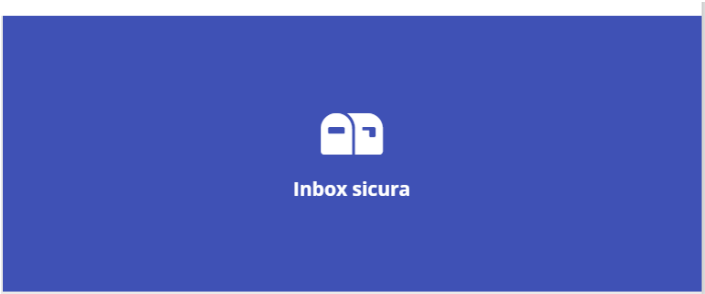
Ti suggeriamo di accedere all'interno della Inbox sicura (Casella postale) e prendere nota del numero della segnalazione e della Password. Questo ti consentirà di effettuare il login in un secondo momento.

Il numero della tua segnalazione è : Q2XH-BF4



Hai aperto una Inbox - casella postale sicura. Per accedere alla casella postale, devi utilizzare la password che hai appena digitato. Se si dimentica una delle credenziali (Numero della segnalazione / Password), è necessario inviare una nuova segnalazione. Per motivi di sicurezza e di tutela dell'anonimato, non possiamo recuperarle.

11. The SB will proceed to start the investigation as described in the relevant Protocol. You will be able to view the progress of your report by accessing the Software from the link <https://ibfservizi.integrityline.com/>, and clicking on the "Inbox Sicura" button.



12. The software will ask you to enter the report number and your password

Accesso alla segnalazione

Quando crei la Inbox, ti sarà assegnato un numero della segnalazione e sceglierai una password. Usa il numero della segnalazione e la password per accedere alla Inbox e vedere se hai ricevuto domande. Se lo desideri, tutte le nostre comunicazioni saranno anonime.

Numero della segnalazione

Password di accesso

13. From the page that opens you can check any replies from the SB and manage communications

