



TECNOFIRMA S.p.A.

REPORTING OF VIOLATIONS

“WHISTLEBLOWING”

December 2023

INDICE

THE PURPOSE	pag. 3
SCOPE OF APPLICATION	pag. 4
REFERENCES	pag. 5
DEFINITIONS	pag. 6
RESPONSIBILITIES	pag. 8
SIGNAGE	pag. 10
INTERNAL SIGNALING CHANNEL	pag. 11
Person Responsible for the Channel	
Characteristics of the Internal Reporting Channel	
Characteristics of Reporting and Anonymous Reporting	
Iteration of Management of Reporting through the Internal Reporting Channel	
Retention of Documentation	
Reporting Obligations	
EXTERNAL CHANNEL OF REPORTING	pag. 17
PUBLIC DISCLOSURE	pag. 18
OBLIGATION OF CONFIDENTIALITY	pag. 19
PROTECTION OF PERSONAL DATA	pag. 21
PROTECTION AND SUPPORT MEASURES	pag. 22
Prohibition of Retaliation	
Support Measures	
Limitation of the reporter's liability	
PENALTY REGIME	pag. 24

This procedure is adopted by TECNOFIRMA S.p.A. (hereinafter the "Company") in compliance with the provisions of Legislative Decree No. 24 of March 10, 2023 (hereinafter the "Legislative Decree 24/2023") in force as of March 30, 2023, which transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, concerning the protection of persons who report breaches of national or European Union regulatory provisions (c. d. whistleblowing directive) that come to their attention in the context of their work, which are detrimental to the public interest or the integrity of the public administration or private entity.

The expression whistleblower means a person who reports, to the bodies entitled to intervene, violations or irregularities committed to the detriment of the public interest and the administration to which he or she belongs.

All employees of the Company have an obligation to promote and ensure the integrity of the actions carried out by the Company. Therefore, in the event that an action or omission committed by an employee of the Company in the performance of his or her work duties may constitute a violation of national or European Union regulatory provisions (as better specified in the "Definitions" section), it is necessary to report it. To this end, the Company has activated, and makes available to employees and third parties, an easily accessible channel (Whistleblowing platform) for submitting and reporting a violation.

This procedure is subject to approval by the Company's Board of Directors, as is the identification of the organizational roles involved in the process of handling whistleblowing reports and the related responsibilities.

To supplement the provisions of this procedure, reference is made to Legislative Decree 24/2023 and the channel activated by the Company: <https://tecnofirma.trusty.report>.

This procedure is part of the measures implemented by the Company to ensure compliance with regulatory provisions and ensure compliance with the behavior criteria established by the Company's Code of Ethics.

SCOPE OF APPLICATION

This procedure applies to any report of information on violations (as better specified in the paragraph "Definitions") acquired within the work context, to be understood as an employment relationship with the organization or professional/work performance, present or past, if detrimental to the public interest or the integrity of the public administration or private entity, made through the appropriate reporting channels made available by the Company.

Excluded from the scope of this procedure are:

- disputes, claims or requests related to an interest of a personal nature that relate exclusively to individual labor relations, i.e., labor relations with hierarchically subordinate figures;
- violations related to national security, as well as to procurement related to defense or national security aspects;
- violations mandatorily regulated by European Union or national acts (ref. Directive 2019/1937 and Legislative Decree 24/23) that already guarantee appropriate reporting procedures.

REFERENCES

- Legislative Decree No. 24 of March 10, 2023;
- Directive (EU) 2019/1937;
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree 196/2003 and ss.mm.ii.);
- ANAC Guidelines on the Protection of Persons Reporting Violations of Union Law and Protection of Persons Reporting Violations of National Law Provisions - Procedures for the Submission and Management of External Reports.

DEFINITION

- **"Reports"**: any written, oral, or exposed communication in an interview, including anonymously, containing information about violations;
- **"violations"**: administrative, accounting, civil or criminal offenses; violations of organization and management models; offenses falling under certain areas of union law (public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health consumer protection; protection of privacy and protection of personal data and security of networks and information systems); acts or omissions detrimental to the financial interests of the European Union and the free movement of goods, persons, services and capital; acts or omissions detrimental to the financial interests of the **"informazioni sulle violazioni"**: tutte le informazioni, tra le quali i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria/contabile intrattiene un rapporto giuridico ed anche gli elementi informativi riguardanti condotte volte ad occultare tali violazioni;
- **"information on violations"**: all information, including well-founded suspicions, concerning violations committed or which, on the basis of factual evidence, could be committed in the organization with which the reporting person or the person making the report to the judicial/accounting authority has a legal relationship and also information elements concerning conduct aimed at concealing such violations;
- **"internal reporting"**: communication of "reports" through the prepared internal reporting channel;
- **"external reporting"**: written or oral communication of information about violations, submitted through the external reporting channel;
- **"public disclosure"**: making information about violations in the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people;
- **"whistleblower"**: an individual who makes a report or public disclosure of information about violations acquired within his or her work context.

- **"work context"**: present or past work or professional activities through which, regardless of the nature of such activities, a person acquires information about violations and within the scope of which he or she may be at risk of retaliation if he or she reports or publicly discloses or reports to the judicial or accounting authorities
- **"person involved"**: a natural or legal person mentioned in the report as a person to whom the violation is attributed or as a person otherwise implicated in the reported violation;
- **"channel IT manager"**: an external person identified by the Company responsible for the technical operation of the channel;
- **"channel manager"**: an internal person identified by the Company responsible for the management of the channel and reporting with organizational and functional autonomy;
- **"retaliation"**: any conduct, act or omission, even if only attempted or threatened, carried out by reason of the report and closely related to it, the report to the judicial or accounting authority or public disclosure and which causes or may cause the reporting person or the person who made the report, directly or indirectly, unjust damage;
- **"follow-up"**: the action or actions initiated by the person entrusted with the management of the reporting channel;
- **"acknowledgement"**: communication to the reporting person of information regarding the action taken or intended to be taken on the report including the measures planned or taken or to be taken and the reasons for the choice made;
- **"platform"**: an internal reporting channel adopted by the Company (as further specified in section "Internal Reporting Channel") to transmit information on violations;

RESPONSABILITIES

The Channel Manager, through the use of the platform:

- makes available, including through this procedure and information published on the platform, clear information about the channel, procedures and prerequisites for making internal reports;
- issues acknowledgement of receipt of the report to the reporting person within the prescribed time limit;
- assesses the criteria for processability of the report;
- shares the report with internal stakeholders, defined within this procedure, the initiation of any investigations, their outcome and feedback to the reporting person;
- transmits feedback to the reporter about the closure of the report handling process;
- maintains interlocutions with the reporting person and, where appropriate, manages the request for additions and the execution of any in-depth interviews with the reporting person, if requested;
- files and maintains documentation on the report within the regulatory timeframe;
- coordinates and monitors the investigation phase with assigned internal functions/external teams;
- shares the report with internal stakeholders, defined within this procedure, the initiation of any investigation, its outcome and feedback to the reporter;
- identifies improvement plans to prevent the recurrence of reportable events;
- manages the activities resulting from any public disclosures in the cases provided for;
- ensures compliance with the principle of confidentiality.

Whistleblower:

- transmits reports in compliance with this procedure;
- is required to provide circumstantial information related to what is reported.

The **IT Manager of the channel**:

- ensures the technical operation of the channel.

The **Legal Representative**:

- interloquisce con ANAC in caso di eventuale segnalazione esterna o attivazione di attività ispettive da parte di ANAC.

The **Board of Directors**:

- approves this procedure together with the structure of related organizational roles;
- ensures compliance with the measures for the protection of the reporting person.

REPORTERS

Whistleblowers may report:

- employees;
- the self-employed and collaborators who perform their activities at or for the Company;
- the freelancers;
- consultants;
- the shareholders;
- the directors;
- the providers of services for third parties in any capacity (regardless of the nature of such activities) even without remuneration;
- trainees, including unpaid ones;
- individuals who perform functions of administration, management, control, supervision or representation, even if the relevant activities are performed in a de facto and not de jure capacity.

Also included in this category are all those persons who, for any reason, become aware of wrongdoing within the work environment of the Company, or:

- when the employment relationship has not yet begun;
- during the probationary period;
- upon termination of the relationship.

INTERNAL REPORTING CHANNEL

prevention and detection of violations. This choice responds to the principle of fostering a culture of good reporting and corporate social responsibility as well as improving one's organization.

The internal reporting channel involves the written mode through the platform accessible from the link: <https://tecnofirma.trusty.report/>

and from the page: <https://www.tecnofirma.com/whistleblowing>

The internal reporting channel guarantees the confidentiality of the identity of the reporter, the persons involved and otherwise mentioned in the report as well as the content of the report and the related documentation submitted, which can be supplemented at a later date.

Characteristics of the Internal Reporting Channel

The Company's internal reporting channel is supported by the "Trusty.report" platform, is web-based and usable from all devices (PC, Tablet, Smartphone).

IT management of the internal reporting channel is carried out by:

Trusty AG, Riedstrasse 7, 6330 Cham, CH (support@trusty.report).

The database is encrypted and hosted on virtual servers in high-security data centers located in the EU.

Data entered into the platform are secreted in the logical partition dedicated to the Company and subjected to scripting algorithm before storage. Security is ensured by secure communication protocols.

The platform provides at the end of the entry of the report (regardless of whether it is anonymous or not) a username and password, randomly and automatically generated by the IT platform, which cannot be reproduced, and with which the reporter can at any time view the processing status of his or her report and interact with the person in charge through a messaging tool.

INTERNAL REPORTING CHANNEL

The report can be viewed and handled only by authorized individuals. The responsible party has unique credentials for access, expiring every 3 months. Password policy adheres to international best practices.

Data Retention is governed by predefined deadlines with automatic reminders to the channel manager who will proceed, upon expiration, to delete the data.

The processing of personal data must always take into account and comply with the obligations under the GDPR and Legislative Decree 196/2003 and ss.mm.ii. The Company, as the data controller through the internal reporting channel, is required to carry out a prior analysis of the organizational design including the fundamental assessment of the possible impact on data protection (Article 35 of the GDPR).

Characteristics of Reporting and Anonymous Reporting

It is necessary that the report be as comprehensive as possible in order to enable the analysis of the facts by those responsible for receiving and handling reports. In particular, it is necessary to be clear:

- the circumstances of time and place in which the fact that is the subject of the report occurred;
- the description of the fact;
- the generalities or other elements that make it possible to identify the person to whom the reported facts are attributed.

Information about reported violations must be truthful. Mere suppositions, poorly reliable indiscretions (so-called rumors), as well as news in the public domain, erroneous information (with the exception of genuine error), manifestly unfounded or misleading, or if merely harmful or offensive, are not considered such. On the other hand, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the identity of the perpetrator of the facts.

It is also useful for the reporter to provide documents that may give elements of substantiation of the reported facts, as well as an indication of other individuals potentially aware of the facts.

Anonymous reports, where substantiated, are equated with ordinary reports and in that case considered within the scope of this procedure. The protections of the reporter, if subsequently identified, and retention obligations are also considered within the scope of this procedure.

Iter di Gestione della Segnalazione tramite il Canale interno

The reporter submits the report through the dedicated internal channel.

The reporter activates the report through the above link in written mode by completing a guided form.

Receipt of the report by the person in charge of the channel initiates the report management process.

Upon receipt of the report, the responsible party shall provide an acknowledgement to the reporter within 7 days of receipt of the report and the acknowledgement of the report.

The person in charge of the channel proceeds with an initial verification regarding the correctness of the procedure followed by the reporter and the content of the report, both with reference to the scope defined by this procedure (so-called inherent nature of the content of the report) and its verifiability based on the information provided. If the report does not fall within the scope of this procedure, the channel manager formalizes the outcome of the check and communicates it to the reporter within a reasonable time (no more than 3 months) and files the report.

If it is necessary to acquire additional evidence/information/documentation, the channel manager will contact the reporter through the platform. In case the reporter does not respond/provide further documentation, within 3 months of the request for supplementary information, the channel manager proceeds with the filing of the report by notifying the reporter.

If it is not necessary to acquire additional elements, the channel manager will assess, on a case-by-case basis, with the Company whether and which corporate function should be appropriately involved for the relevant analysis and any consequent measures, always in compliance with the principle of confidentiality, and how to initiate the investigation phase.

INTERNAL REPORTING CHANNEL

The person in charge of the channel, upon completion of the investigation, prepares a final report in order to proceed with the feedback to the reporter. The feedback to the reporter must be submitted within 3 months from the date of acknowledgement of receipt or the expiration of the 7-day period from the submission of the report.

Only in exceptional cases, if the complexity of the report requires it, or in view of the reporter's response time, the channel manager, having promptly informed the reporter before the deadline, with appropriate justification, may continue the investigation phase for as long as necessary, and giving the reporter periodic updates.

In case of defamation or slander, ascertained by conviction even in the first instance, the Company shall proceed with sanction proceedings against the reporter.

It is specified that, from the receipt of the report until its closure, any person in a situation of conflict of interest must refrain from making decisions in order to ensure compliance with the principle of impartiality.

Retention of Documentation

Internal reports and all related attached or supplemented documentation are kept, with appropriate digital chain of custody, for as long as necessary for the processing of the report itself.

In case, documentation is retained only for a time period identified as a maximum of 5 years from the date of the communication of the final outcome of the reporting procedure.

In all cases mentioned above, it is necessary that the procedure for keeping internal reports and related documentation, complies with EU and national guarantees on the processing of personal data as well as with the prepared measures on the right to confidentiality.

Information obligations

Information on the channel, procedures and prerequisites for making reports are displayed in the workplace (company bulletin boards) through the publication of this procedure and made known to persons who, although not frequenting the workplace, have a legal relationship with the Company through publication on the appropriate web page of the Company's institutional website:

<https://www.tecnofirma.com/whistleblowing>

The Company activates its internal whistleblowing channel after hearing the workers' representatives (BOD).

EXTERNAL REPORTING CHANNEL

Upon the occurrence of the following conditions, the whistleblower may proceed with a report to ANAC through an external channel:

- in cases where in the relevant work context, activation of the internal reporting channel is not mandatory or the channel itself has not been activated or does not comply with regulatory requirements;
- when the reporter has already filed an internal report it has not been followed up;
- if the whistleblower has reasonable grounds to believe that by filing an internal report, the report is not effectively followed up or that the report itself will result in retaliation against the whistleblower;
- if the reporter has a well-founded reason to believe that the reported violation may pose an imminent or obvious danger to the public interest.

The external body entitled to receive external reports is ANAC according to the modalities and procedures appropriately adopted by the latter.

PUBLIC DISCLOSURE

In via residuale e subordinata, il segnalante potrà procedere con una divulgazione pubblica nei seguenti casi:

- quando ha già previamente effettuato una segnalazione interna ovvero esterna, ovvero ha effettuato direttamente una segnalazione esterna senza aver ricevuto riscontro nei termini previsti;
- nel caso in cui ha fondato motivo di ritenere che la violazione costituisce un pericolo imminente o palese per il pubblico interesse;
- quando ha fondato motivo di ritenere che la segnalazione esterna comporta il rischio di ritorsioni ovvero può non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possono essere occultate o distrutte prove oppure in cui vi è fondato timore che chi ha ricevuto la segnalazione può essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

OBLIGATION OF CONFIDENTIALITY

All reports and their attachments shall not be used beyond the time necessary to follow up on them.

It is provided that the identity of the reporter together with any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed without the express consent of the reporter to persons other than those competent to receive or follow up the reports, expressly authorized to process such data pursuant to Articles 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and Article 2-quaterdecies of the code on the protection of personal data under Legislative Decree No. 196 of June 30, 2003, as amended and supplemented.

The Company shall protect the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated by reason of the report itself, in compliance with the same guarantees provided in favor of the reporting person.

Mitigating circumstances for the protection of the right to confidentiality include:

- within the framework of criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure: the obligation of secrecy of the acts of the preliminary investigation is imposed until the time when the suspect does not have the right to have knowledge of them and, in any case, not later than the closure of this phase;
- within the scope of the proceedings established at the Court of Accounts, the identity of the whistleblower may not be disclosed until the close of the preliminary investigation stage;
- within the framework of disciplinary proceedings, the identity of the reporter may not be disclosed where the allegation of the disciplinary charge is based on investigations separate and additional to the report, even if consequent to it;
- where the charge is based, in whole or in part, on the report and the knowledge of the identity of the reporting person is indispensable for the defense of the accused, the report will be usable for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to reveal his or her identity;

OBLIGATION OF CONFIDENTIALITY

- in cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, written notice will be given to the reporter of the reasons for the disclosure of confidential data when the disclosure will also be indispensable for the defense of the person involved.

Given the vigor of the mitigations just listed, the person involved, upon his or her request, shall also be heard through a cartular procedure through the acquisition of written comments and documents.

Confidentiality obligations include:

- the subtraction of the report and the documentation attached to it from the right of access to administrative acts provided for in Articles 22 et seq. of Law No. 241/1990 and from the generalized civic access provided for in Articles 5 et seq. of Legislative Decree No. 33/2013;
- administrations and entities involved in the management of reports guarantee confidentiality during all stages of the reporting process, including the possible transfer of reports to other competent authorities.

PROTECTION OF PERSONAL DATA

All processing of personal data, including communication between competent authorities, is carried out in accordance with:

- of Regulation (EU) 2016/679;
- of Legislative Decree No. 196 of June 30, 2003, as amended.

Disclosure of personal data by institutions, bodies or organs of the European Union is carried out in accordance with Regulation (EU) 2018/1725.

The processing of personal data relating to the receipt and management of reports is carried out by the owner, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by preliminarily providing the appropriate information to the reporting subjects and the persons involved as well as by taking appropriate measures to protect the rights and freedoms of the data subjects.

<https://tecnofirma.trusty.report/data-privacy>.

Data subjects can find information summarizing their rights and how to exercise them in the dedicated section of the Whistleblowing platform:
<https://tecnofirma.trusty.report/data-privacy>.

.

PROTECTION AND SUPPORT MEASURES

Sono previste adeguate misure per proteggere i segnalanti dalle ritorsioni. Appropriate measures are in place to protect whistleblowers from direct retaliation and indirect retaliation.

The protection measures apply if at the time of reporting the reporting person had reasonable grounds to believe that the information about the reported violations was true (see section "Characteristics of Whistleblowing and Anonymous Reporting"), fell within the objective scope, and the reporting procedure was followed.

In the case of defamation or libel, established by conviction even in the first degree, protections are not guaranteed.

The protective measures also apply:

- to persons in the same work environment as the reporting/whistleblowing person who are related to them by a stable emotional or kinship relationship within the fourth degree;
- to co-workers of the reporting/denouncing person who work in the same work environment as the reporting/denouncing person and who have a usual and current relationship with that person;
- to entities owned by the reporting/whistleblower person or for which the same persons work, as well as entities that work in the same work environment as the said persons.

Divieto di Ritorsione

I soggetti enumerati nel paragrafo "Responsabilità" non possono subire alcuna ritorsione. A titolo esemplificativo e non esaustivo si considerano "ritorsioni": il licenziamento, la sospensione o misure equipollenti; la retrocessione di grado o la mancata promozione; il mutamento di funzioni.

Gli atti assunti in violazione del divieto di ritorsione sono nulli.

Nell'ambito di procedimenti giudiziari o amministrativi ovvero in caso di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati nei confronti dei soli soggetti segnalanti, si presume che gli stessi siano stati posti in essere a causa della segnalazione. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione è del soggetto che ha posto in essere gli atti ritorsivi.

PROTECTION AND SUPPORT MEASURES

Whistleblowers may notify ANAC of retaliation they believe they have experienced, whether attempted or contemplated.

The ANAC informs the National Labor Inspectorate, for measures within its competence.

Support Measures

The reporter may turn to Third Sector entities on the list published on the ANAC website. These are entities that carry out activities in the general interest for the non-profit pursuit of civic, solidarity and socially useful purposes ("promotion of the culture of legality, peace among peoples, nonviolence and unarmed defense; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of general interest activities, promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups") and that have entered into agreements with ANAC.

The support measures provided consist of information, assistance and advice free of charge on how to report, the protection from retaliation offered by national and European Union regulatory provisions, the rights of the person involved, and the terms and conditions of access to legal aid.

Limitation of liability of the Whistleblower

Provisions are made for the absence of liability (including civil or administrative liability) for anyone who discloses or disseminates information about violations:

- covered by the obligation of secrecy,
- related to copyright protection,
- of provisions relating to the protection of personal data,
- offending the reputation of the person involved or reported,

whether, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the violation and the reporting was made consistent with the conditions for protection.

PROTECTION AND SUPPORT MEASURES

In addition, protective measures include:

- the rights to make a report and related protections cannot be restricted in a contractual way;
- the exclusion of all other liability, including civil and administrative liability, for acquiring or accessing information on violations, except where the conduct constitutes a crime;
- the exclusion of any other liability with regard to conduct, acts, omissions made if related to the report and strictly necessary to reveal the violation or, in any case, not related to the report.

DISCIPLINARY REGIME

The disciplinary system adopted by the Company pursuant to Article 6, paragraph 2, letter e), of Legislative Decree 231/2001, and referred to in the General Part of the 231 Model, provides for sanctions to be applied against those whom the Company ascertains to be responsible for the offenses referred to:

- commission of retaliation or proposed adoption, obstruction of reporting (even attempted) or violation of confidentiality obligations,
- failure to establish reporting channels, failure to adopt procedures for handling them, or procedures that do not comply with the requirements of the decree or failure to carry out verification and analysis of reports,
- civil liability of the reporting person for defamation or slander in cases of willful misconduct or gross negligence, unless the person has already been convicted, also at first instance, for the crimes of defamation or slander;

as well as against anyone who violates this procedure.

For the same offenses, ANAC may intervene with the application of administrative pecuniary sanctions (from € 500 up to € 50,000) if the same offenses are ascertained.