Co-funded by the European Union

SAFE—IN

Strengthening Actions against Fraud: Empowering whistleblowing directive compliance

Deliverable 5.1

Guidelines and good practices handbook

Grant agreement no° 101140591
Project - SAFE-IN
Submission date
2024-03-19

Responsible author(s)
ANCI LOMBARDIA

This project has received funding from European Union's Union Anti-Fraud Programme under grant agreement no Project 101140591 — SAFE-IN. The content of this report reflect only the author's view. The European Commission is not responsible for any use that may be made of the information it contain.

Short Summary

The "Guidelines and Good Practices Handbook" deliverable outlines the objectives, guidelines, and practical measures of the "SAFE-IN" project, a pivotal initiative designed to enhance whistleblowing systems by Legislative Decree No. 24/2023 in Italy. This decree, which transposes the EU Whistleblowing Directive (2019/1937) into national law, not only ensures adherence to European standards but also strengthens the broader framework for organizational accountability and fraud prevention.

The primary aim of the documents is to strengthen the implementation of whistleblowing systems within public and private organizations. This ambition arises from the growing recognition that an effective whistleblowing mechanism is central to safeguarding ethical governance and transparency. By addressing gaps in compliance, the "SAFE-IN" project creates a structured pathway for organizations to align with evolving regulatory demands and public expectations.

The “Guidelines and Good Practices Handbook” sets out several interconnected goals that highlight its comprehensive scope:

- Development of Reporting Mechanisms: The document emphasizes the need for robust and compliant internal reporting systems, which are critical for the early detection of misconduct.
- Regulatory Adherence: Ensuring alignment with both EU and national regulations is not merely an obligation but a cornerstone of fostering trust in organizational practices.
- Promoting Ethical Culture: A culture of integrity, transparency, and accountability is advocated as a proactive measure to reduce unethical behaviour.
- Whistleblower Protection: Safeguards against retaliation are underscored to ensure that individuals feel empowered and secure when reporting misconduct.
- Best Practices Adoption: Standardizing procedures across diverse sectors ensures consistency and effectiveness in addressing violations.

The document identifies a clear set of beneficiaries, targeting those directly responsible for the implementation and maintenance of whistleblowing systems:

- Public and Private Sector Personnel: This includes staff within public administrations, publicly controlled entities, and small and medium enterprises (SMEs). These stakeholders are essential to embedding whistleblowing mechanisms into everyday organizational practices.
- Internal Reporting Managers: Roles such as HR managers, compliance officers, and anti-corruption officers are highlighted as pivotal actors in managing the systems.
- Whistleblowers and Related Stakeholders: Employees, contractors, suppliers, and volunteers who report misconduct are prioritized for protection and support.

Beyond these direct groups, the document also benefits organizations themselves by offering operational and compliance support to align with the whistleblowing regulations. The intentions of the document are strategic and multidimensional:

- Regulatory Compliance: By providing a structured framework, this document enables organizations to meet the legal requirements of Legislative Decree No. 24/2023, ensuring legal accountability.
- Operational Support: Practical guidance for establishing secure and efficient reporting channels is offered, highlighting the technical and procedural aspects of whistleblowing.
- Cultural Shift: The initiative extends beyond compliance to encourage ethical decision-making, active citizenship, and justice as fundamental principles within organizations.
- Whistleblower Protection: The document places a strong emphasis on confidentiality and anti-retaliation measures to create a safe environment for those reporting misconduct.

To achieve these objectives, the Guidelines delve into practical recommendations, offering detailed insights into establishing internal and external reporting channels, safeguarding data, and implementing ongoing training programs. Furthermore, it highlights the indispensable role of senior leadership in fostering a culture of transparency and trust. Leaders are positioned as key drivers in embedding these principles across organizational structures, ensuring the long-term effectiveness of whistleblowing systems..

INDEX

January 3, 2025

1. Introduction

Whistleblowing was introduced in Italy through specific legislation at the end of 2017 with Law No. 179. This law provided comprehensive regulation for public administration and introduced certain provisions for private sector organizations with a management and control organizational model under Legislative Decree No. 231/2001.

Law N. 179/2017 was superseded by the transposition of the European Directive on Whistleblowing (No. 1937/2019). The new law, Legislative Decree No. 24/2023 (hereinafter referred to as the Regulation), implements the EU Directive No. 2019/1937 of the European Parliament and Council of October 23, 2019, concerning the protection of persons reporting breaches of Union law and national provisions.

The new Regulation imposes obligations on public and private organizations, including the requirement for all public entities to establish internal procedures for handling reports. Private sector entities with an organizational model under Legislative Decree No. 231/2001, as well as all private organizations with at least 50 employees, are subject to the same obligations.

For public administrations and companies with at least 250 employees, these obligations came into effect on July 15, 2023. For private organizations with 50 to 249 employees, the obligations became effective on December 17, 2023.

The Regulation emphasizes the central role of the National Anti-Corruption Authority (ANAC), which now acts as the National Whistleblowing Authority, overseeing both the public and private sectors. Pursuant to Article 10 of the decree, ANAC has issued an initial version of guidelines on whistleblowing, approved under Resolution No. 311 on July 12, 2023. These guidelines aim to ensure uniform and effective application of whistleblowing regulations and provide further guidance for entities required to implement them.

On November 7, 2024, ANAC released a proposed updated version of the guidelines to complement and integrate previous guidance for external reporting channels. The updated version provides instructions on managing internal reporting channels and establishes a standardized structure for handling reports in both public and private sectors.

The guidelines were developed based on monitoring conducted by ANAC in 2023 on the state of whistleblowing implementation, as well as consultations with institutional stakeholders, trade associations, and civil society. Key topics include:

- Internal reporting channels and methods for reporting.
- Duties and activities of managers.
- Obligations for staff in both public and private sectors.

- Personnel training.
- Support roles played by Third Sector organizations.

As part of its efforts to raise awareness on whistleblowing, ANAC allowed citizens and stakeholders to provide feedback (by December 9, 2024) through a questionnaire. The submitted feedback will be published and made available to the public.

Beyond ANAC's guidelines, several trade associations (both entrepreneurial and professional) have developed documents providing practical guidance tailored to the various organizations subject to the whistleblowing regulations. Examples include:

1. "Whistleblowing Operational Guide" (December 7, 2023) by the Labor Consultants Foundation.
2. Updated Behavioral Norms for Non-Listed Companies' Boards of Statutory Auditors, by the National Council of Chartered Accountants and Auditors (CNDCEC).
3. "New Whistleblowing Regulations and Impact on Legislative Decree 231/2001", a research document by CNDCEC (October 2023).
4. Position Paper (October 10, 2023), "The Role of Supervisory Bodies in Whistleblowing," by the Association of Supervisory Bodies under Legislative Decree 231/01.
5. Operational Guide for Private Entities (October 2023) by Confindustria: "New Whistleblowing Regulations."

These documents will likely be updated to reflect changes introduced in ANAC's revised guidelines.

2. Purpose of the document

This document does not yet include the content of ANAC's new guidelines (as they are not yet published) and can be considered a reference framework for drafting procedures/policies for managing reports under Legislative Decree No. 24/2023. Being a framework, it must be adapted to the specific reality of each organization and coordinated with existing compliance systems (e.g., the Three-Year Anti-Corruption Prevention Plan and/or the Integrated Activity and Organization Plan, the Organizational, Management, and Control Model pursuant to Legislative Decree 231/2001, etc.).

Based on the results of the "SAFE-IN" project, this document was created to support public and private organizations in implementing Legislative Decree No. 24/2023. Specifically, following an analysis of the regulatory context and skills needs identified during training activities, the project team defined key methodological steps that organizations can consider when formalizing a procedure/policy for managing the reporting system.

These steps draw on good practices that emerged during educational workshops involving representatives of various stakeholders, including public administration entities and publicly controlled bodies (the so-called public sector) and Small and Medium Enterprises (SMEs, the so-called private sector).

This information is presented schematically and concisely, yet organizations are encouraged to reflect on broader themes such as justice, legality, and active citizenship. These reflections foster the development of positive social attitudes, autonomy in judgment, and critical thinking. Only by doing so can those subject to the legislation diversify acceptable behaviours from unacceptable ones, thereby rejecting and mitigating inappropriate conduct.

In this context, the commitment of senior management is crucial. Senior leaders should actively participate in defining how information about internal and external reporting channels should be communicated to potentially affected individuals (e.g., publication in a clearly visible section of the organization's website) and in promoting continuous training initiatives on legislative developments and related procedures. Such efforts help to foster a culture of integrity and responsibility within the organization.

3. Beneficiary

This document is intended for the personnel of public administrations, publicly controlled entities, and SMEs involved in the development and maintenance of the process for managing reports, as well as in the implementation, monitoring, and review of the whistleblowing system.

It is primarily addressed to the so-called "managers of internal reporting channels," along with other public/private organization personnel involved in the whistleblowing system. These may include:

- Human Resources/HR Managers,
- Senior officials managing corruption-prone areas,
- Other individuals responsible for internal controls, such as:
    - **Anti-Corruption and Transparency Officers** (RPCT) as per Law 190/2012,
    - **Supervisory Bodies** (OdV) under Legislative Decree 231/2001,
    - Internal Auditors,
    - Compliance and Risk Managers,
    - Data Privacy Officers,
    - Independent Evaluation Bodies (OIV) under Legislative Decree 33/2023,
    - Project managers for initiatives funded under the PNRR (National Recovery and Resilience Plan),
    - Boards of Statutory Auditors,
    - Independent directors, etc.).

4. Who Can Report Through Internal Reporting Systems?

The new whistleblowing regulation encourages anyone who, in the context of their work activities, becomes aware of violations committed by or on behalf of the organization to report such misconduct.

The goal is to facilitate the communication of information related to violations identified during work activities. The scope of potential whistleblowers is therefore broad. Formalized procedures/policies aim to effectively identify possible "whistleblowers" when they report illegal conduct concerning the entity.

Reports can be submitted in accordance with established procedures by the following categories of individuals:

- Employees,
- Collaborators,
- Suppliers, subcontractors, and their employees and collaborators,
- Freelancers, consultants, and self-employed workers (e.g., consultants supporting administrations and entities in implementing projects funded by EU funds),
- Volunteers and interns, whether paid or unpaid,
- Shareholders or individuals with administrative, managerial, supervisory, monitoring, or representative roles (e.g., board members, including non-executive members, members of OIVs or OdVs, student representatives in university governance bodies, etc.),
- Former employees, collaborators, or individuals who no longer hold one of the above-mentioned positions,
- Individuals undergoing selection, probation, or whose legal relationship with the organization has not yet commenced.

The procedure must also ensure the protection of facilitators, i.e., individuals who assist whistleblowers in the reporting process while operating in the same work context. Facilitators' identities must be kept confidential[1].

[1] The facilitator could be a colleague who also has the qualification of trade unionist if he assists the informer on his behalf, without spending the union acronym. It should be noted that if, on the other hand, he assists the whistleblower using the union code, he does not play the role of facilitator. In this case, the provisions on consultation of trade union representatives and the suppression of anti-union behaviour remain unaffected.

5. What Types of Misconduct Are Considered in Reporting Procedures?

Reports may concern illegal activities encountered in the context of the reporter's work activities. They may also include well-founded suspicions of violations of the law or risks of such violations.

The whistleblower is not required to fully demonstrate the occurrence of an offense, but reports should be as detailed as possible to allow the recipients to investigate the reported facts. At the same time, whistleblowers are discouraged from conducting personal investigations that could expose them to risks.

The types of violations that can be reported include:

1. **Violations of national laws:**
    - Criminal, civil, administrative, or accounting offenses not expressly linked to violations of EU law.
    - Offenses defined as predicate crimes under Legislative Decree 231/2001 or breaches of organizational and management models established by this decree.
2. **Violations of EU regulations and laws**, including:
    - Offenses violating EU regulations specified in Annex 1 of the Decree, and all national provisions implementing these regulations, including those not explicitly listed in the annex.
    - Violations related to:
        - Public contracts,
        - Financial services and anti-money laundering measures,
        - Product safety and compliance,
        - Transport safety,
        - Environmental protection,
        - Radiation protection and nuclear safety,
        - Food and feed safety, animal health and welfare,
        - Public health,

        - Consumer protection,
        - Privacy and data protection,
        - Security of networks and information systems.
    - Acts or omissions that harm the EU's financial interests, as defined by Article 325 of the TFEU.
    - Actions that compromise the internal market, affecting the free movement of goods, people, services, and capital (Article 26, Paragraph 2, TFEU).
    - Abusive practices or actions that violate EU law objectives, as interpreted by the European Court of Justice (e.g., abuse of dominant market positions).

The law explicitly excludes reports already governed by specific sectoral laws (e.g., financial services, anti-money laundering, transport safety, environmental protection) or those related to national security, defense, or public safety. Personal grievances (e.g., related to employment contracts) or disputes involving hierarchical relationships within an organization are also excluded unless they affect the public interest or the organization's integrity.

Reports should include the following key elements to ensure they are admissible:

- Identifiable information about the whistleblower (e.g., name, surname, date of birth, and a contact method for updates).
- Detailed circumstances of the reported event (e.g., time, place, and specific facts).
- Identification of the person(s) responsible for the misconduct.

Supporting documents and evidence, along with information about others who may have knowledge of the reported facts, should be included whenever possible.

The procedure should also clarify the relationship between the whistleblowing regulation and special sectoral regulations, particularly regarding overlapping requirements.

6. Who Receives and Manages Reports?

In public sector organizations, the Anti-Corruption and Transparency Officer (RPCT) is responsible for receiving and managing reports. The RPCT may be supported by a designated team within the organization.

In the private sector, the choice of the entity to be entrusted with the management of the reporting channel (cd. Internal Channel Manager) is left to the discretion of the institution, taking into account the activity carried out and the related responsibilities, as well as the organizational structure it has established, provided that the following autonomist requirements are guaranteed: i) impartiality, that is to say, the absence of any bias or prejudice against the parties involved in whistleblowing reports, with a view to ensuring fair handling of the reports and free from internal or external influences which could compromise their objectivity; ii) independence, that is autonomy and freedom from influence or interference by management, in order to ensure an objective and impartial analysis of the report. It is undeniable that this figure must also have a certain authority within the organization and above all be recognized as a "reliable" figure to whom to transmit the reports. The following are some considerations arising from the most accredited best practices regarding the identification of the figure of the Internal Channel Manager**:**

- **An individual within the company**, this role can be held by the anti-corruption officer, if present, or by the heads of internal audit or compliance functions rather than in the case of medium and small enterprises, in the absence of such figures, The role of a manager of the alert could be entrusted to an entity with no operational tasks (e.g. responsible for legal functions or human resources, etc.)

- **Office/Body within the company**, this role could be fulfilled by a committee composed, for example, of those responsible for control functions (compliance or Internal Audit) and some of the other business functions that can handle reporting in an appropriate and diligent manner (think, for example, legal functions or human resources functions, the anti-corruption officer or Ethics Committees, as well as the Supervisory Body, if monocratic, or a member of it, if collegial, with further duly formalized assignment)[2].

[2] In any case, even if the FOE was not entrusted with the handling of alerts, it is appropriate that it be involved in the process of handling whistleblowing reports by regulating the necessary information flows, in compliance with the confidentiality obligations, in light of the relevance, also for the purposes of 231, of the violations reportable under the Decree.

- **Office outside the company,** in which case the companies will have to verify that it has the necessary autonomy, independence and professionalism. In this respect, the external party must possess, among others, resources and specialist knowledge that guarantee the adoption of technical and organisational measures to ensure confidentiality, data protection and secrecy. The relations between the parties, moreover, will have to be regulated by appropriate service contracts which, besides regulating the services provided between the parties, must include appropriate levels of service and control. It would also be appropriate that support staff are identified within the entity itself, also with a view to ensuring the Manager a better knowledge of the organizational context in which he is called to carry out his activity.

If the organisational choice made by the institution is to identify a body that receives and manages reports other than the OdV, it would be desirable that the procedure regulates the process of connection between the OdV and the Manager of the Internal Channel, in coordination with a new paragraph of the updated Model 231 dedicated to reports of violations of the same Model 231 and/ or, more generally, of D.lgs. 231/01. This is because the OdV must always be able to monitor the operation and compliance with Model 231, even when it does not deal with the management of the reporting channel. In particular if the OdV is not identified as a Manager, it could receive for example: i) immediate information on relevant reports in terms 231 so that, in the exercise of its supervisory activity, be able to share any observations and participate in the investigation or otherwise follow its progress; ii) a periodic update on the overall activity of handling alerts, also not 231, in order to verify the functioning of the whistleblowing system and propose to the institution any need for improvement. **It would also be appropriate for the procedure to clarify whether the internal reporting channel under D.lgs. 24/23 managed by an entity other than the OdV is alongside other channels for reporting offences 231 rather than using a single reporting channel.**

With regard to the identification of the internal channel manager for public sector entities, required to appoint a RPCT, art. 4 co. 5 of the D.Lgs. 24/2023 identifies in this figure the entity to entrust the management of the internal channel. With the obligation, as regards the use of external entities, for local authorities to verify beforehand, with negative result, the presence in the staff of entities capable of fulfilling the tasks provided for by the legislation. Significant novelty compared to the previous legislation is the possibility of "sharing" for small institutions the internal reporting channel and its management:

- These are the municipalities other than provincial capitals with less than 50 employees;

-These are private sector entities that have employed, in the last year, an average of employees with fixed-term or indefinite employment contracts, not exceeding 249.

In any case, the public organization is desirable that appoint the Manager of the Internal Channel

with a specific organizational act heard the representations or trade union organizations referred to in art. 51 of the Legislative Decree n. 81/2015, while the private one defines such figure within Model 231, if any, and in any case appoint it by a special resolution of the Board of Directors, after hearing the representatives or organizations referred to in art. 51 of Legislative Decree 81/2015.

The RPCT or Manager of the Internal Channel appointed by the Body, receives the reports and talks with the reporting person to clarify and deepen what received. The dialogue with the reporting person continues even during the detection phases. The Internal Channel Manager or the office, after an initial assessment, carry out an activity of verification of the reported information, also requesting specific information from other offices and functions within the organization. The recipient provides regular feedback to the reporting person and, at the end of the assessment activity, reports on the outcome of the assessment activities.

The report of the outcome shall not include any reference to personal data relating to the individual reported.

Possible outcomes that may be communicated to the reporting person include:

- Correction of internal processes and first level control devices
- Initiation of disciplinary proceedings
- Transfer of the results of the verification activities to the Public Prosecutor's Office (and/or the Court of Auditors in case of tax damage)
- Filing for lack of evidence

Fundamental to regulate within the procedure how to manage possible reporting activity upwards in compliance with the governance of the organization (e.g. Social Organs in companies, Political Steering Body in Public Administration) with regard to the reports received and what emerged from their analysis, always safeguarding the confidentiality of the informer, also considering the suggestions of the National Council of Accountants and Accountants on the occasion of the update of the "Rules of conduct for the board of statutory auditors of unlisted companies[3]. The report that is mistakenly sent to the superior may not be treated as a report under the whistleblowing legislation, since the latter does not have the same confidentiality obligations as the recipient.

[3] The following new principle has been introduced: "5.5. Relations with the supervisory body: for the purpose of carrying out its supervisory activities, the Board of Statutory Auditors obtains information from the supervisory body regarding the function assigned to it by law in order to monitor the adequacy, on the functioning and compliance with the model adopted ex Law No. 231/2001. The board of auditors verifies that the model provides terms and conditions for the exchange of information between the supervisory body and the administrative body and the board itself".

Fundamental to the procedure, how to manage the transmission of the report to a person other than the Manager of the Internal Channel.

It is also considered inadvisable to inform the management of the company about a possible conflict of interest in handling alerts; it would be advisable to inform the management of the the Internal Channel Manager abstaining, due to a conflict of interest, from reporting, by inviting the latter to contact the substitute or, where applicable, transferring the report to the substitute [4].

7. Internal Reporting Channels

The organization provides whistleblowers with various internal channels for reporting violations in accordance with the regulations. Reports can be made in either oral or written form.

The regulations outline three types of reporting mechanisms:

a) Reporting through an internal channel within the organization.

b) Reporting through an external channel managed by ANAC (National Anti-Corruption Authority).

c) Public disclosure (in addition to the option to file complaints with judicial or accounting authorities when relevant).

Internal channels are particularly encouraged as they are closer to the origin of the issues being reported.

It is advisable that written reports be submitted and managed through a **dedicated digital platform** to ensure stringent security measures and a higher level of protection for personal data, both during the submission and management of reports. This approach facilitates:

- Encryption of data at rest.
- Secure and confidential communication with the whistleblower.

The confidentiality of reports must be safeguarded both technologically and organizationally. Encrypted digital platforms are intended as tools for interaction and storage but not for the entire management of the report.

[4] Therefore, recourse to ANAC would be a residual remedy if the dispute is not settled in the internal procedure.

Such platforms may include a **questionnaire** to guide whistleblowers through the reporting process using open- and closed-ended questions, some of which may be mandatory, with the ability to attach supporting documents. Upon submission, the whistleblower may receive a **unique code**, allowing them to access their report, engage in two-way communication with the recipient, exchange messages, and provide additional information.

All information on the platform must be encrypted and accessible only to authorized personnel responsible for receiving the reports.

It is essential to specify within the organization's procedures that **other written reports (outside the platform) cannot be managed**. If such reports are submitted, the recipient should, where possible, request the whistleblower to resubmit the report through the digital platform.

If no digital platform is adopted, alternative methods must ensure confidentiality. A **double-envelope protocol** may be used:

1. The first envelope contains the whistleblower’s identification details and a copy of their identification document.
2. The second envelope contains the report, thereby separating the whistleblower's identity from the report itself.
3. Both envelopes are placed in a third, sealed envelope marked "confidential," addressed to the report handler.

Oral reports may be submitted through one of the following methods:

- Telephone lines or voice messaging systems.
- A direct meeting, upon the whistleblower’s request, within a reasonable timeframe.

It is recommended to invite the whistleblower to contact the Internal Channel Manager to arrange a telephone interview or, if necessary, a personal meeting.

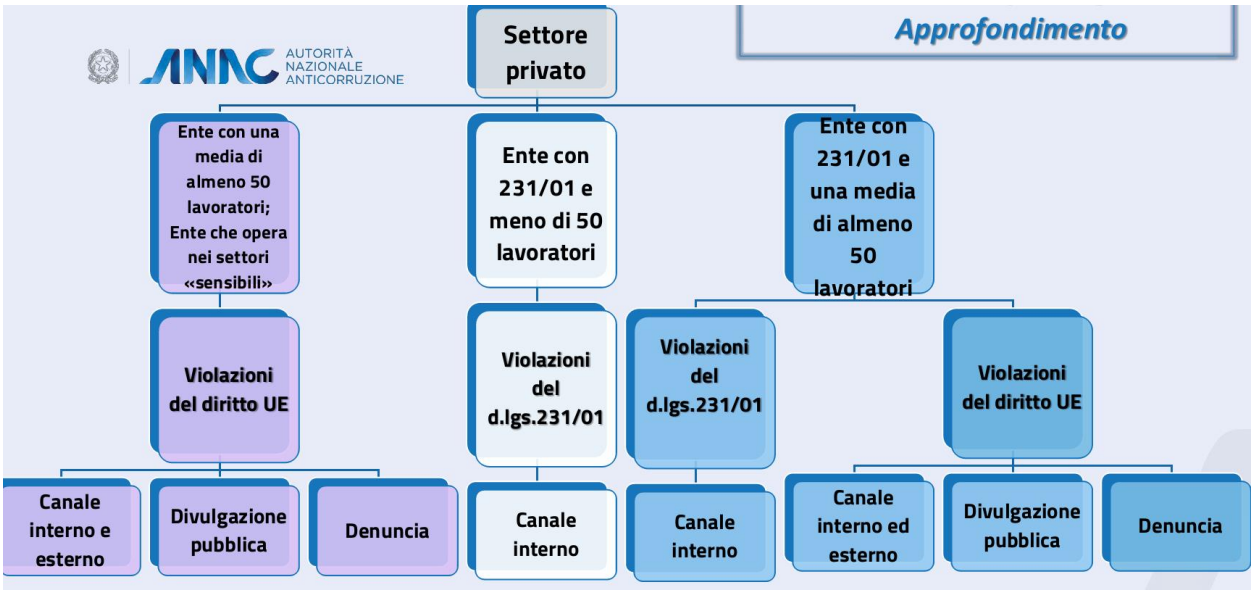
Oral reports should be transcribed into a written record, and the transcript must be signed by the whistleblower for it to be processed.

It is important to note that oral reports do not provide the same level of technological confidentiality as reports submitted via encrypted digital platforms.

The following is a summary, presented in tabular form, based on the ANAC document *“Whistleblowing Regulations: Updates Introduced by Legislative Decree No. 24/2023 Implementing European Directive No. 1937/2019”*, which outlines "WHAT AND HOW TO REPORT" in the public and private sectors.

.


ANTICORRUZIONE
SETTORE PUBBLICO
- VIOLAZIONI DEL DIRITTO INTERNO (come sopra elencate)
- VIOLAZIONI DEL DIRITTO UE (come sopra elencate)
CANALE INTERNO
CANALE ESTERNO
DIVULGAZIONI PUBBLICHE
DENUNCIA ALL'AUTORITA' GIUDIZIARIA O CONTABILE


AUTORITÀ NAZIONALE ANTICORRUZIONE
Settore privato
Approfondimento
Ente con una media di almeno 50 lavoratori; Ente che opera nei settori «sensibili»
Ente con 231/01 e meno di 50 lavoratori
Ente con 231/01 e una media di almeno 50 lavoratori
Violazioni del diritto UE
Violazioni del d.lgs.231/01
Violazioni del d.lgs.231/01
Violazioni del diritto UE
Canale interno e esterno
Divulgazione pubblica
Denuncia
Canale interno
Canale interno
Canale interno ed esterno
Divulgazione pubblica
Denuncia

8. Timelines for Managing Reports Through a Digital Platform

At the end of the reporting process, the platform provides a receipt code to confirm that the report has been submitted and acknowledged by the Internal Channel Manager.

Within 7 days of the transmission of the alert, the Internal Channel Manager confirms to the reporting person that the report has been taken over and invites the reporting person to monitor its report on the platform and to make itself available to respond to any requests for clarification or further information. Within 3 months from the day of reporting, the Internal Channel Manager shall provide the reporting person with a confirmation of the verification activities carried out to verify the information reported in the report. The feedback provided within 3 months may coincide with the outcome of the verification activities. If these are not concluded, the Manager of the Internal Channel invites the reporting person to keep monitoring the evolution until the final outcome of the same. Of course, if this process is run without the platform's support, it is necessary that the Manager guarantees the same timing and above all ensures a smooth and continuous communication with the reporter in order to make its presence and attention felt in the management of the report.

9. Confidentiality and Anonymity

The Internal Channel Manager is required to handle reports while maintaining their confidentiality. Information regarding the identity of the whistleblower, the individual(s) reported, and any other persons mentioned in the report must be treated according to principles of confidentiality. Similarly, all details contained within the report itself must also be handled with the utmost confidentiality.

The identity of the reporting person may not be disclosed without his or her consent. The right of access to the relevant information by the persons concerned is also denied. The only reason for possible disclosure of the identity of the person who is issuing the alert may be where the verification documents are submitted to an ordinary or accounting prosecutor and knowledge of this is necessary for the purposes of the right of defence during a Ordinary judicial or accounting proceedings before the Court of Auditors. Anonymous reports are also possible. Entities receiving anonymous reports via internal channels are still required to record and maintain records in accordance with the general retention criteria applicable in their respective jurisdictions, thus making it possible to trace them, in the case where the whistleblower, or who has lodged a complaint, informs ANAC that he has been subjected to retaliatory measures due to that anonymous report or complaint.

The Manager of the Internal Channel, based on the guidelines of the Governance can decide whether to process them or not; also this aspect would be desirable to regulate within the Procedure. In any case, alerts shall be treated according to the same principles of confidentiality. However, in the case of anonymous alerts, the receiving entity has no knowledge of the identity of the reporting person and could unintentionally expose him during the detection activities.

10. The handling of personal data

Reports received, investigation activities and communications between the reporting person and the Internal Channel Manager are documented and stored in accordance with confidentiality and data protection requirements.

The receipt and management of internal reports determine the processing of personal data of persons involved in various ways in the reported facts. Therefore, in the definition of the internal reporting channel, particular attention must be paid to compliance with the regulation on personal data protection (EU Regulation n. 679/2016, c.d. GDPR, and D.lgs. n. 196/2003, c.d. Privacy Code), so that the processing of the reports following their submission is carried out in accordance with this legislation. The legislation contains several provisions on the protection of personal data, aimed at defining the role of the entities that activate the internal reporting channel and of the parties involved in receiving and managing reports (art. 12, co. 2 and art. 13, co. 4, 5, and 6) and, on the other hand, to direct the setting of the models for receiving and managing reports (art. 12, co. 1 and art. 13, co. 1, 2, 3 and 6 and art. 14)[5].

Alerts contain personal data and may be processed and maintained only for the time necessary to process them: this time includes analysis, assessment and reporting of findings, as well as any additional time for possible additional comments. In no case will the alerts be kept for more than 5 years after the result of the investigation has been communicated to the person who is issuing the alert. Once the activities of handling the alert have been completed, the operator shall keep both the report and the related documentation for the time necessary to process the report, but no longer than five years from the date of communication of the final outcome of the reporting procedure, In accordance with the principle of minimisation. Regarding access to personal data, these are known only by the recipient and, if indicated in a specific organizational act, by members of the support staff for the management of the report.

During the verification activities, the Internal Channel Manager may share with other functions of the institution previously anonymised and minimized information in relation to the specific activities of responsibility of these latter.

[5] For more details on the following topics, please refer to paragraph "7. Processing of personal data" of the Confindustria Guidelines": a) the framework for processing dependent on the receipt and management of a report; b) the identification and formalization of the privacy organigram relating to the internal reporting channel; c) the setting up and implementation of processing operations following alerts.

11. Safeguards and protections

The person referred to in the alert as being responsible for the suspected offence is subject to similar identity protection measures as the reporting person and other persons mentioned in the alert.

In addition to the protection of the confidentiality of the identity of the reporting person and of the persons mentioned in the report, as well as of the content of the report, there are other forms of protection that must be guaranteed.

The reporting person is guaranteed protection against any form of retaliation or discrimination that he or she might suffer as a result of and following a reporting. Retaliation means any act or omission, threatened or actual, direct or indirect, connected with or resulting from reports of actual or suspected wrongdoing, that causes or may cause physical, psychological, reputation damage to the person, economic losses.

Possible forms of discrimination include:

- or dismissal, suspension or equivalent measures;
- or demotion or failure to advance;
- change of job, change of place of work, reduction of salary, change of working time;
- the suspension of training or any restriction on access to it;
- Notes of merit or negative references;
- disciplinary measures or other sanctions, including pecuniary penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavourable treatment;
- the non-conversion of a fixed-term employment contract into an indefinite one, where the worker had a legitimate expectation of such conversion;
- the non-renewal or early termination of a forward contract;
- or damage, including to the person's reputation, economic or financial prejudice, including loss of economic opportunities and income;
- Listing on inappropriate lists based on a formal or informal sectoral or industrial agreement, which may result in the person being unable to find employment in the

sector in the future;

- the early conclusion or cancellation of a contract for the supply of goods or services; the cancellation of a licence or permit; the request to undergo psychiatric or medical examinations.

It is therefore necessary to integrate the Disciplinary System, considering that the legislation requires that it be adapted by providing for sanctions against those responsible for violations for which ANAC applies administrative fines to the Institution (as detailed in the next paragraph). It would therefore be desirable to assess whether the measures already provided for in the disciplinary system are adequate and sufficient to penalize the violations indicated by the new whistleblowing legislation; these are the following cases: i) the commission of any retaliation - to be understood as a behaviour, act or omission, even if only attempted or threatened, which is made because of the report (the complaint to the judicial or accounting authority or the public disclosure) - which causes or may cause directly or indirectly, unfair harm to the reporting person (or the person who filed the complaint or made a public disclosure) and/or other entities specifically identified by the standard; ii) failure to establish reporting channels, the failure to adopt whistleblowing procedures in accordance with the law or even the failure to carry out verification and analysis activities regarding the reports received; iii) the implementation of actions or behaviour by which the alert was obstructed or attempted to be obstructed; iv) the breach of the obligation of confidentiality. In addition, the legislation provides that disciplinary sanctions must be imposed if it has been established the responsibility of the informer, even by judgment of first instance, for the offences of defamation or slander (or in any case for the same offences committed in connection with a complaint) or its civil liability in cases of intent or gross negligence.

12. Sanctions

Legislative Decree n.24/2023 provides for administrative sanctions, irrogable by the National Anti-Corruption Authority in case of violation of the rules on whistleblowing.

The sanctions specifically concern the following cases: possible retaliation against reporting persons, breaches of confidentiality, boycott of a reporting attempt, failure to take up an alert or insufficient investigation initiated as a result of the alert. Abuse of the reporting system is also punishable, with possible sanctions for someone who slanders or defames another subject through the procedure. The Institution may take disciplinary action against the persons responsible for these conduct.

The activity of ANAC to ascertain any retaliation against the reporting person leads to possible sanctions against the responsible entity. In this case, as well as in cases where an individual has obstructed a report or has violated the obligation of confidentiality in handling a report, penalties can range from 10,000 to 50,000 euros.

Other sanctions profiles concern the absence of procedures for handling reports or non-compliance with the legislation for institutions that are required to provide such channels; Failure to take up reports received is also punishable. The penalties also range from EUR 10,000 to 50,000. A different type of penalty and much smaller (from 500 to 2,500 euros) is provided against the reporting person responsible for slander or defamation or other responsibilities related to the reporting or complaint

The Authority's sanction-type proceedings are modelled on a regulation prepared by the Authority, adopted by Resolution n. 301 of 12 July 2023, which provides for a real investigation with request for pleadings, documents and deductions, With hearings of the whistleblower, alleged discriminator and witnesses

13. External channels for reporting

Outside the internal channel for the transmission of reports, the legislation also allows external reports to the National Anti-Corruption Authority and public.

Without prejudice to the preference for the internal channel, the legislation provides the possibility of making a report through the external channel of ANAC, if one of the following conditions is met: i) in its working context, the activation of the internal channel is not foreseen as mandatory or, if planned, it has not been activated; ii) the alert was not followed up; iii) has reasonable grounds to believe that if he made the internal report it would not be followed up or would face retaliation; (iv) has reasonable grounds to believe that the breach may constitute an imminent or apparent danger to the public interest. In implementation of the power/duty assigned to it, ANAC has regulated, in the Guidelines and in the appropriate Regulation, the modalities for the presentation and management of external reports, providing that they can be made only by natural persons entitled under Decree-Law 24/23 (instead, they may not be made, for example, by representatives of trade union organizations). The procedures for reporting to the National Anti-Corruption Authority are available on the dedicated page of the A.N.AC website: anticorruzione.it/-/whistleblowing.

There are additional conditions under which a reporting person may make a public disclosure, namely: i) an internal report that the administration/entity has not complied with within the prescribed time period has been followed by an external report to ANAC which, in turn, has not provided a response to the informer within a reasonable time; ii) the person has already made a direct external report to ANAC which, However, it has not provided the informer with a response to the measures planned or taken to follow up on the alert within a reasonable time; iii) the person directly makes a public disclosure because he or she has reasonable grounds to believe that on the basis of concrete circumstances and therefore not merely on the basis of mere conjecture, that the breach may pose an imminent or obvious danger to the public interest; iv) the person directly makes a public disclosure because he has reasonable grounds to believe that the external reporting may entail a risk of retaliation or may not be followed up effectively. This is a very sensitive issue for companies, due to the potential for damage to the institution of a complaint made without any justified grounds or substantiated evidence. The potential adverse effects may also be exacerbated by the fact that disclosure can be made not only through print media but also through dissemination means capable of reaching a large number of people, such as social networks and new communication channels (e.g. Facebook, Twitter, etc.), which are not supervised by specific disciplines, ethical rules and controls by appropriate supervisory authorities. **Within the procedure, it could be clarified that public**

disclosure can only be carried out through mass media «overseen» by sector regulations and with the opportunity to better define the concept of «good cause», in order to reduce the level of discretion of the reporting authority, for example by providing that it must be explained/justified by the reporting authority. Only for the Public Administration, this procedure should also be coordinated with the recently updated provisions of the Code of Conduct. Art. 11-ter to paragraph 2 requires the public employee to "refrain from any intervention or comment" that may affect prestige, decorum or image of its own administration or P.A. in general belonging to the administration or public administration in general; paragraph 3 then provides that in order to ensure the confidentiality of communications relating to the service, should normally be avoided "public conversations through the use of digital platforms or social media".