ANDERSEN®

June 2026

&Compliance Risk Management

New regulations and practices for data governance and business risk management

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Contributors: **Nicolò Bottura**, **Elisa D'Arrigo** and **Edoardo Vittorio Lazzaro**

D.Lgs. 231/2001

Failure to Comply with Whistleblowing Regulations: Non-Compliance and Liability Risks

Nearly three years after the entry into force of Legislative Decree No. 24/2023, many organizations continue to underestimate the obligations introduced by the whistleblowing framework. However, implementing **compliant reporting channels** and adopting appropriate procedures are not merely formal requirements; they are essential tools for preventing misconduct and safeguarding corporate integrity.

Organizations subject to the legislation must establish internal reporting channels that ensure the **confidentiality** of the whistleblower's identity, the individuals involved, and the content of the report. They must also define **a clear and traceable process** for handling reports, in compliance with applicable data protection regulations.

Failure to comply may expose organizations to significant consequences. Legislative Decree No. 24/2023 grants the Italian National Anti-Corruption Authority (ANAC) the power to impose **administrative fines** on entities that **fail** to establish the required reporting channels or that adopt procedures not meeting legal standards.
Similar sanctions may apply where organizations obstruct the submission of reports or engage in retaliatory actions against whistleblowers.

In addition to regulatory penalties, organizations should not overlook the potential **reputational and operational impacts**. The absence of an effective reporting system may hinder the organization's ability to promptly identify unlawful conduct, operational irregularities, or regulatory breaches, potentially resulting in financial losses and reputational damage.

For companies that have adopted an organizational, management, and control model pursuant to Legislative Decree No. 231/2001, compliance with whistleblowing regulations is a key component of the **internal control system**.
Periodic assessments of the adequacy of reporting channels and related procedures therefore represent not only a compliance obligation but also a best practice in corporate governance and risk prevention.

Privacy | AI | Cyber

Handling whistleblowing reports and processing personal data: the risk of a data breach is becoming increasingly real!

The handling of whistleblowing reports involves new and complex challenges for corporate security, placing the protection of personal data at the top of the priority list.

In this scenario, the risk of a data breach is no longer a remote possibility, but a very real threat. In fact, reports may contain, in addition to common personal data (identifying information of the whistleblower and the subject of the report), also **special categories of personal data** (so-called "sensitive data") such as details on alleged violations, names of individuals involved, documentary evidence, health-related data, as well as, for example, data regarding sexual orientation, political, philosophical, and religious views.
If this data is compromised due to **unauthorized access, cyberattacks, or simply human error**, the consequences for the organization are significant.

A data breach can result not only in heavy **fines** from the Data Protection Authority but also in **reputational damage** that undermines the trust of employees and stakeholders. It goes without saying that no employee will use reporting channels if they fear their identity might be exposed. To mitigate this risk, companies must adopt an approach based on "privacy by design and by default." It is essential to implement **encrypted communication channels**, restrict access to only formally authorized individuals, and provide ongoing training for staff responsible for handling reports.
It should also be noted that in the event of a data breach, the General Data Protection Regulation (GDPR) requires notification to the supervisory authority **within 72 hours of becoming aware of the incident** if the risk to individuals' rights and freedoms is high. Only through rigorous **governance**, encrypted IT systems, and a corporate culture focused on **security** can the management of reports be transformed into a secure asset, thereby reducing the risk of data breaches.

Risk Management

Unsubstantiated reports: the risks for the person making the report

The **whistleblowing** system is a key tool for promoting transparency and preventing wrongdoing within organisations.

However, the protection afforded to whistleblowers is not unlimited: the safeguards provided for by law do not apply to those who make unfounded reports with **intent or gross negligence**.

Internally, the company may initiate **disciplinary proceedings** for the misuse of the reporting channel, up to and including the application of sanctions provided for under the company's disciplinary system.

The person reported may take action to obtain **civil compensation for damages** caused by the unfounded report.

Furthermore, unfounded reports may constitute the criminal offences of **defamation** or **slander**.

For the offences mentioned above, in the event of a criminal **conviction** or a finding of civil liability, the whistleblower **loses the protections** provided for by whistleblowing legislation and is also subject to a disciplinary sanction.

The reporting channel does not require certainty of wrongdoing, but presupposes that the whistleblower acts in **good faith**, on the basis of reliable and verifiable information.

Using the whistleblowing channel for retaliatory, personal or self-serving purposes exposes to **risks** that may be far more serious than the benefits that the legislation grants to those who report correctly.