

Whistleblowing in the private sector: building a system that works

Opinion article by Burcin Atakan, Partner, and Elton Mata, Manager, Advisory, Forensic Services, Deloitte Romania



In recent years, whistleblowing has progressed considerably into becoming a key aspect of an organization's corporate governance. It started with the adoption of the EU Whistleblowing Directive (2019/1937) and was gradually transposed into national laws, including Romania's Law no. 361 in December 2022. This legal framework sets clear obligations for establishing secure reporting channels, ensuring confidentiality, and protecting whistleblowers from retaliation.

Since 2022, EU member states have progressed at different speeds in implementing these rules. While most have completed their transposition, the maturity of the systems and legal enforcement varies widely.

For private sector companies, legal compliance is only the starting point. An effective whistleblowing framework is not about "ticking

a box” — it’s about building a trusted environment where employees, contractors, and even suppliers feel safe to speak up, and where the organization can respond effectively. But how can organizations ensure that their whistleblowing system is effective? Below are various core aspects which companies can use in implementing a robust reporting system.

Implementing an effective reporting system

a) Choose the right channels

A one-size-fits-all approach rarely works. Employees should have access to multiple reporting options depending on the nature of the business: a secure online portal, a dedicated phone line, and the possibility of face-to-face reporting, the latter under confidential circumstances for protecting the whistleblower’s identity.

For smaller companies, anonymity options are essential to reduce fear of retaliation. Larger organizations often integrate multilingual and 24/7 availability to cover global teams, therefore, the risk of whistleblower identification is considerably lower.

b) Ensure accessibility and awareness

A reporting channel effectiveness relies on its reachability and familiarity. The better a company communicates to its employees or partners their policies, the existence of a safe reporting channel where misconduct can be disclosed, the more effective the system will be. How can companies educate their employees? By launching internal awareness campaigns using intranet posts, posters, and onboarding sessions, By training managers to

encourage, and not discourage reporting, by using plain and simple language in policies for ease of understanding.

c) Guarantee confidentiality and security

Reporting systems should be encrypted, and the access should be strictly limited to authorized personnel handling the cases. An important feature to the effectiveness of a whistleblowing system is the appointment of independent professionals handling reported cases, be it internal or external parties of the company.

The organization should decide who leads the process: compliance, HR, internal audit, or an independent function. As an example, multinational companies ensure local laws are met in each jurisdiction depending on the requirements, while keeping central oversight within headquarters.

e) Stay compliant with data protection

Every organization should keep in mind and respect GDPR principles. Information should be processed with transparency and lawfulness. Data should be stored in a secure environment within EU.

Moreover, only necessary information related to the specific subject should be requested and processed.

Handling reports properly

Step 1: Acknowledge quickly

The EU Directive requires confirmation within seven days — but beyond compliance, it shows the whistleblower they've been

heard, and necessary steps are being taken to remediate the situation.

Step 2: Triage the case

Assess severity and urgency. High-risk issues (criminal conduct, threats to health or safety) require immediate escalation. Each issue reported should represent high importance and should be treated seriously. Negligence can lead to potential financial losses and reputational impact.

Step 3: Assign an independent investigator

Avoid conflicts of interest, particularly in cases involving senior management. Independent internal auditors or external specialists can ensure neutrality. Although the decision on assigning the teams to handle the investigation relies solely on the organization, it is vital that the investigation team be independent from any parties involved in the allegations reported by a whistleblower.

Step 4: Protect the whistleblower

Anti-retaliation measures are not just legal requirements — they're essential for maintaining trust. From a broader perspective, whistleblower protection promotes transparency, accountability, and integrity in both the private and public sectors.

Step 5: Investigate thoroughly

Collect evidence systematically: documents, interviews, digital forensics. Maintain confidentiality but ensure relevant stakeholders are informed as needed. Forensic expertise may be

required in various cases when investigating delicate situations of any kind of misconduct.

Step 6: Provide feedback

Even if details are limited for legal reasons, inform the whistleblower about the outcome or the next steps. A better relationship with the whistleblower can help bring forward more details of the misconduct reported, making the investigation process much easier.

Step 7: Implement remediation

Address root causes. This may involve disciplinary action, policy changes, training, or internal controls improvement. Remediation actions should focus on the collective good of the company and employees, while sustaining integrity and fairness in any changes which the company may undergo due to the misconduct faced.

Step 8: Continuous improvement

Regardless of the field of activity or subject in review, any organization's scope should be constant growth and development of their internal policies, procedures and surely their culture.

Final thoughts

In conclusion, an effective whistleblowing policy and setup can bring significant benefits to an organization. It provides the company with early detection of problems such as fraud, harassment, or safety hazards, allowing them to be addressed before escalating into unresolvable issues. It also serves as a

safeguard against regulatory breaches, reducing the risk of fines and legal liability. Beyond compliance, such a system strengthens workplace culture. When employees feel safe to speak up, they tend to be more engaged and loyal. In the same way, a strong and trustworthy reporting mechanism helps decline the potential occurrence of misconduct within the organization.