UNIVERSITY OF TURIN

IMPLEMENTING THE WHISTLEBLOWER DIRECTIVE

A Comparative Report on Italy, Romania, Estonia, Latvia and Poland

COMPARATIVE ANALYSIS BASED ON THE FIVE WAKE-UP NATIONAL REPORTS

8 MAY 2026

PROJECT PARTNERS

SUPPORTED BY

Co-funded by the European Union

Executive Summary

This comparative report assesses the practical implementation of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (the "Whistleblower Directive") in five Member States: Italy, Romania, Estonia, Latvia and Poland. It is based on the five national reports produced under the WAKE-UP project between January and April 2026. The five reports rely on partly different methodologies — desk research and freedom-of-information requests in Romania, qualitative interviews with channel managers and stakeholders in Italy (twelve interviews), Latvia (twenty), Poland (ten) and Estonia (sixteen) — but converge on a single, consistent diagnosis: across all five countries, the legal framework is now broadly aligned with the Directive, while the practical functioning of the system reveals a substantial implementation gap.

The five Member States transposed the Directive at very different speeds. Latvia adopted its first whistleblowing law as early as 2018 and updated it in 2022 and again in 2026; Romania transposed the Directive in 2022 (Law 361/2022); Italy in 2023 (Legislative Decree 24/2023); Estonia in May 2024; and Poland — the last EU country to comply — in June 2024, after three years of delay and under the threat of severe financial sanctions imposed by the Court of Justice of the European Union. These different starting points shape the maturity of national practices, but they do not translate into proportionally different outcomes: even Latvia, with the longest experience, registers approximately one third of submissions as well-founded whistleblowing reports, and shares with its peers the central problem of underuse.

Five common findings emerge from the comparison. First, the volume of reports is generally low and unevenly distributed across institutions, with a sizeable share of public bodies recording zero substantive reports. Second, the typology of submissions is dominated by interpersonal conflicts, HR grievances and procedural noise rather than by the integrity violations that the Directive was designed to surface. Third, confidentiality is the cornerstone of protection in all five countries, while structured anti-retaliation monitoring, support measures and access to legal aid remain underdeveloped. Fourth, cultural barriers — the "snitch" stigma in Poland, Estonia and Romania, organisational closure and the preference for hierarchical channels in Italy and Latvia — represent the single most consistently cited obstacle. Fifth, civil society and trade unions are weakly integrated into the whistleblowing architecture in all five countries, with the partial exceptions of Italy (third-sector entities listed in a dedicated register) and Latvia (Transparency International Latvia / Delna).

At the same time, the reports identify country-specific patterns that resist over-generalisation. Italy and Romania have invested in centralised authorities (ANAC and ANI) and in sophisticated digital reporting platforms; Latvia is alone in not allowing anonymous whistleblowing reports under the Whistleblowing Law (although KNAB accepts anonymous "violation reports"); Poland exhibits a striking "technological regression" toward analog channels, sealed envelopes and physical safes, driven by distrust of internal IT departments; Estonia has deliberately limited the scope of its act to breaches of EU law, which generates confusion among employees and limits the practical value of the system for typical domestic concerns.

The report concludes with four sets of recommendations addressed to EU institutions, Member States, obliged entities and civil society. Common priorities include clarifying the relationship between whistleblowing and ordinary administrative complaints; ensuring substantive examination of credible anonymous reports; investing in awareness, training and de-stigmatisation campaigns; strengthening monitoring of retaliation; providing free legal aid and psychological support; and creating cross-institutional fora to exchange anonymised case studies and standardise practice.

1. Introduction

1.2 Purpose and rationale of the comparative analysis

Directive (EU) 2019/1937 was adopted to overcome the previous fragmentation of national whistleblower protection regimes and to set a common minimum standard across the European Union. Five years after its entry into force, and in some Member States only a few months after national transposition, it has become possible — and necessary — to look beyond the legal text and assess whether, and to what extent, the system is actually functioning. The five national reports that form the empirical basis of this comparative analysis were drafted with that aim: to capture both the formal architecture and the lived practice of whistleblowing in the public administration, in state-owned enterprises, in healthcare and academic institutions, in private companies and, where relevant, in the third sector.

The purpose of the present comparative report is twofold. First, to map the convergences and divergences between the five national systems, identifying patterns that recur across very different legal cultures and institutional settings, as well as features that remain country-specific. Second, to translate the resulting picture into a set of actionable policy recommendations addressed to the actors best placed to close the implementation gap, from the European Commission down to the responsible officers handling reports in a small municipality.

1.2 Scope: countries, time horizon, sectoral coverage

The five Member States covered — Italy, Romania, Estonia, Latvia and Poland — were selected to represent a meaningful diversity of legal traditions (civil-law systems with different transposition strategies), administrative cultures (centralised vs. decentralised) and institutional histories (founding Member States and post-2004 enlargement countries, including three with a post-Soviet legacy that strongly affects organisational culture and trust). The analysis covers the period from the adoption of the relevant national law to the cut-off date of the underlying national reports (March 2026). Sectorally, the comparison includes central and local public administration, ministries, state-owned enterprises, universities, hospitals, large municipalities and small ones, and — to a lesser but still significant extent — the private sector and civil society organisations.

1.3 Methodology and sources

The present comparative report is a secondary analysis of the five national reports produced under the WAKE-UP project. The national methodologies are not fully aligned. The Romanian report rests primarily on desk research — official institutional reports and press releases of the National Integrity Agency (ANI), monitoring reports of the National Anti-Corruption Strategy (SNA) 2021–2025 — supplemented by formal requests for information of public interest sent to ministries, county councils, city halls and universities. The Italian, Latvian, Polish and Estonian reports are based on qualitative semi-structured interviews with people responsible for managing whistleblowing channels, complemented by analysis of legal sources and publicly available institutional data. The Italian sample comprises twelve interviews, the Latvian one twenty, the Estonian one sixteen and the Polish one ten. Romania has acquired information through Freedom of information request.

To produce the comparative analysis, the team harmonised the structure of the five reports into a common analytical grid (legal framework — channels — practice — protection — challenges — strengths) and treated each thematic cluster comparatively, indicating both shared findings and country-specific divergences. Where quantitative data are reported, we cite them with their source and reference period; where the underlying methodology is heterogeneous, we flag the asymmetry explicitly rather than impose artificial comparability.

1.4 Limitations

Three principal limitations affect this comparative exercise and should be made explicit. First, the heterogeneity of national methodologies — particularly between Romania (desk and FOIA) and the four interview-based studies — restricts the depth of strict statistical comparison. Second, the available data largely reflect institutional self-reporting, which tends to underestimate phenomena such as retaliation, informal pressure and the use of informal channels; the absence of cases of retaliation in many institutional records cannot be read as the absence of the phenomenon. Third, the Polish system has been operational only for a few months and the Estonian one since September 2024, so the most recent observations describe an evolving rather than a settled situation.

1.5 Structure of the report

Section 2 sets out the European framework against which national systems are assessed. Section 3 compares the five national legal frameworks, from pre-existing legislation to identified gaps. Section 4 turns to the practical organisation of reporting channels, with particular attention to technological choices and inter-institutional cooperation. Section 5 analyses reporting practice — volumes, topics, outcomes and the “underuse” phenomenon. Section 6 looks at protection in practice, including the treatment of anonymous reports and the effectiveness of judicial remedies. Section 7 brings together the cross-cutting challenges and strengths emerging from the five reports. Section 8 offers a comparative synthesis with country snapshots. Section 9 lays out four sets of policy recommendations, and Section 10 concludes. Annexes provide comparative tables and a methodological note.

2. The European Framework: Directive (EU) 2019/1937 as a Common Reference Point

2.1 Key provisions and rationale of the Directive

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law was the European Union's first horizontal instrument on whistleblowing. Its rationale rests on a simple intuition: persons working for an organisation are usually the first to know about wrongdoing of public concern, and they will only be willing to report it if they are effectively shielded from retaliation. Before the Directive, protection across the EU was fragmented and uneven, with some Member States offering robust safeguards in narrow sectors, others limiting protection to public officials, and a third group having no specific framework at all. The Directive harmonises the picture by setting minimum common standards in three areas: who is protected, how reports are channelled, and how reporting persons are shielded from negative consequences.

The personal scope of the Directive is deliberately broad. Protection covers not only employees, but also self-employed persons, shareholders, members of administrative and supervisory bodies, volunteers, paid and unpaid trainees, and any person working under the supervision and direction of contractors, subcontractors and suppliers. It extends temporally to candidates whose employment relationship has not yet started and to persons whose relationship has ended; it also covers facilitators, third parties connected to the whistleblower (such as colleagues or relatives) and legal entities owned or otherwise associated with the reporting person.

The material scope encompasses breaches falling within specific areas of Union law, including public procurement, financial services and money laundering, product safety, transport safety, environmental protection, radiation protection and nuclear safety, food safety, public health, consumer protection, privacy and personal data, security of network and information systems, breaches affecting the financial interests of the Union and breaches relating to the internal market. Member States are explicitly allowed to extend protection beyond these areas in their national transposition law.

2.2 Common transposition obligations

The Directive imposes a three-tier reporting architecture: internal channels within obliged entities, external channels operated by competent authorities, and public disclosure as a residual option. Public-sector and large private-sector entities (50+ employees, with sectoral exceptions) must establish internal channels and designate impartial persons to handle reports. The Directive sets binding deadlines: acknowledgement of receipt within seven days and feedback within three months (extendable to six in justified cases). It mandates strict confidentiality of the reporting person's identity and prohibits retaliation in all its forms (dismissal, demotion, denial of training, reputational damage and other adverse measures). It introduces the reversal of the burden of proof: in proceedings concerning detriment suffered after a report, the employer must prove that the measure was unrelated to the report. Member States must designate competent authorities, ensure they are independent and adequately resourced, and provide for effective, proportionate and dissuasive penalties for retaliation, breaches of confidentiality and obstruction of reporting.

2.3 The analytical grid used in this comparison

Building on the Directive's structure, this report compares the five national systems along seven dimensions: (i) legal framework and timing of transposition; (ii) personal and material scope; (iii) architecture of reporting channels; (iv) procedural deadlines and confidentiality; (v) protection against retaliation; (vi) competent authorities and oversight; (vii) identified legal and practical gaps. For each dimension, we first look at the formal alignment with the Directive and then at how the rule plays out in practice, drawing on the national reports.

3. Comparative Analysis of the National Legal Frameworks

3.1 Pre-existing national legislation and pathways to transposition

The five Member States arrived at the Directive from very different legal starting points. Italy was a relative pioneer in Europe, having adopted Law 190/2012 (the so-called anti-corruption law) and Law 179/2017, which extended protection to the private sector and introduced the reversal of the burden of proof. The Italian system was already structured around an Anti-Corruption and Transparency Officer (Responsabile della Prevenzione della Corruzione e della Trasparenza, RPCT) and the National Anti-Corruption Authority (ANAC), so the transposition of the Directive — Legislative Decree 24/2023 — represented a systematic consolidation rather than a foundational reform.

Romania had introduced Law 571/2004 on the protection of public authorities personnel reporting breaches of the law, but this framework was limited to the public sector and lacked formal channels and effective protection mechanisms. The Directive was transposed by Law 361/2022, which created a complete reporting system and confirmed the National Integrity Agency (ANI) as the central external authority.

Latvia adopted its first Whistleblowing Law in October 2018, in force from May 2019; this was already an advanced framework that the second Whistleblowing Law of 2022 (in force from February 2022) refined to align fully with the Directive. Further amendments entered into force on 1 March 2026, transferring the national whistleblowing contact point from the State Chancellery to the Corruption Prevention and Combating Bureau (KNAB), introducing liability for the unlawful disclosure of whistleblowing information and broadening the definitions of “performance of work duties” and “associated person”.

Estonia did not have a dedicated whistleblowing statute before the Directive. The Act on Protection of Persons Who Report Work-Related Breaches of European Union Law entered into force on 1 September 2024 — a deliberately narrow legislative choice that anchors protection to breaches of EU law and leaves “purely domestic” matters such as ordinary corruption, fraud and workplace bullying outside the Act unless they overlap with EU rules.

Poland was the last EU Member State to transpose the Directive: the Act of 14 June 2024 on the Protection of Whistleblowers was adopted nearly three years after the deadline of 17 December 2021, after the Court of Justice of the European Union had imposed a lump sum of EUR 7 million and daily penalties of EUR 40,000. The Polish national report describes the resulting law as “a highly technocratic framework” adopted under conditions of “legislative coercion”, with implications that go beyond the legal text and shape implementation throughout the country.

3.2 Timing of transposition and degree of compliance

On paper, all five national laws now align with the Directive’s minimum standards. The chronology, however, is deeply uneven (Latvia 2018/2022/2026 — Romania 2022 — Italy 2023 — Estonia May 2024 — Poland June 2024) and matters in two ways. First, it shapes the time available to develop institutional practice, train responsible persons and accumulate jurisprudence. Latvia and Italy are clearly more advanced in this respect than Estonia and Poland. Second, the political conditions of transposition leave a lasting imprint. The Polish report explicitly attributes the technocratic and somewhat skeletal nature of the Polish Act to the rush to avoid EU sanctions, which precluded a substantive public debate; the same point — adoption as "bureaucratic formality" — would resonate to a lesser extent in Romania, where the legal framework is robust but its take-up at the institutional level remains limited.

3.3 Personal and material scope

The personal scope is largely harmonised across the five countries and broadly aligned with the Directive: in addition to traditional employees, all five frameworks protect self-employed workers, shareholders, members of management or supervisory bodies, volunteers and trainees, persons in the recruitment phase or whose professional relationship has ended, and persons working through subcontractors and suppliers. Italy and Romania explicitly extend the protective umbrella to facilitators, colleagues and other third parties (the so-called "indirect protection"), and to legal entities owned or controlled by the whistleblower; Latvia's 2026 amendments codify the same idea by extending the definition of "associated person" to facilitators and supporting legal entities. Polish law extends protection to persons working under civil-law contracts, including B2B and service agreements that are widely used in the country.

The material scope reveals more meaningful variation. The Italian Decree adopts a horizontal and broad notion of "violation", encompassing administrative, accounting, civil and criminal offences, as long as they harm the public interest or the integrity of the entity concerned. Romania's Law 361/2022 covers disciplinary offences, contraventions and criminal offences across the full Directive list. Latvia's law allows whistleblowers to report violations in any area affecting the public interest, while explicitly identifying 23 fields, from corruption and tax evasion to construction safety, thus representing one of the broadest frameworks among the five. Polish law identifies seventeen main areas; importantly, however, the Polish legislator decided not to include broadly defined labour law in the mandatory catalogue, leaving its inclusion to the discretion of individual entities — a choice strongly criticised by trade unions and labour-law commentators. Estonia goes in the opposite direction: the Act protects only breaches of EU law, with the consequence that purely domestic concerns such as theft, fraud, conflicts of interest in non-EU areas or workplace violence may fall outside the Act's protective scope. Several Estonian interviewees reported confusion among employees about whether their concern actually qualifies for protection.

3.4 Architecture of reporting channels

All five frameworks reproduce the Directive's three-tier architecture: internal channels in obliged entities, external channels operated by competent authorities or civil society organisations, and public disclosure as the last resort. The hierarchy between internal and external channels, however, differs in important respects. The Italian Decree is unusual in expressing a clear preference for internal channels; whistleblowers may turn to the external channel operated by ANAC only when the internal channel is absent or ineffective, when there is a risk of retaliation, or when there is a clear and imminent danger to the public interest. The other four laws follow the Directive's permissive approach, which leaves to the whistleblower the substantive choice between internal and external channels.

Public disclosure is treated everywhere as an extrema ratio, accessible only when prior internal/external channels have failed or in cases of imminent and manifest danger to the public interest. None of the five reports identifies a substantial volume of public disclosure cases.

3.5 Procedural deadlines and confidentiality obligations

On procedural deadlines, the alignment is strict and uniform: acknowledgement of receipt within seven days, feedback within three months extendable to six in justified cases. Latvia adds a refinement: a ten-day deadline (seven days for assessment plus three for communication) for informing the submitter whether the submission qualifies as a whistleblowing report. The Italian, Latvian and Estonian reports confirm broad respect of the seven-day deadline, sometimes even more rapid in practice; the Polish report acknowledges that the seven-day deadline is observed but warns that, in many institutions, the procedure does not progress beyond it because no substantive reports are received.

Confidentiality is codified in similar terms across the five frameworks: the identity of the whistleblower may not be disclosed without consent, except where required by law; access to reporting information is strictly limited to authorised persons. In practice, all five reports describe a combination of pseudonymisation, restricted access, separate registers, audit trails and (where used) end-to-end encrypted platforms.

3.6 Protection against retaliation and reversal of the burden of proof

All five laws prohibit retaliation in broad terms — direct or indirect, formal or informal — and provide a non-exhaustive list of retaliatory measures (dismissal, demotion, reduction of remuneration, denial of training, negative references, harassment and reputational damage). All five embed the reversal of the burden of proof: in any dispute, it is for the employer or the institution to prove that the negative measure was unrelated to the report, although the Estonian formulation — requiring the employer to establish that the measure was "justified" — may leave greater room for retaliatory motives concealed behind ostensibly legitimate decisions.

The differences appear at the level of remedies. Italian and Polish law explicitly provide for the nullity of retaliatory acts and for reinstatement; Italy adds precautionary and injunctive measures, and ANAC is vested with administrative sanctioning powers (including significant fines) for breaches of confidentiality, retaliation and failure to establish reporting channels.

Romania provides for the right to claim compensation and to obtain in-court suspension of measures considered retaliatory. Polish law adds criminal sanctions, including imprisonment of up to 3 years, for intentional obstruction, breach of confidentiality, and physical retaliation. Latvia's 2026 amendments introduce specific liability for the unlawful disclosure of whistleblowing information. Estonia provides penalties for hindering whistleblowing, breaches of confidentiality, and retaliation, but — critically — no sanctions for an organisation's failure to establish a whistleblowing channel or to comply with procedural deadlines, and no specific remedies such as compensation or interim relief.

3.7 Competent authorities and oversight bodies

The institutional architecture of external oversight differs markedly across the five countries. Italy operates a centralised model around ANAC, which acts simultaneously as recipient of external reports, supervisory authority over the implementation of the Decree, and sanctioning body, supported by guidelines that perform a steering and interpretative function. Romania likewise relies on a centralised model anchored to ANI, which manages the external channel and provides counselling to whistleblowers, and on the National Anti-Corruption Strategy (SNA) coordinated by the Ministry of Justice, which complements ANI's role with periodic monitoring. Latvia recently shifted its central contact point from the State Chancellery to KNAB, consolidating expertise within an institution already specialised in corruption prevention.

Poland places the Ombudsman (Rzecznik Praw Obywatelskich) at the centre of the external system, with sectoral ministries and inspectorates also receiving reports; the central role of the Ombudsman generates significant volumes (nearly 690 cases received in the first measurable period of 2025, of which roughly 32% recognised as substantive) but also exposes the office to misdirected complaints and procedural noise. Estonia is the most decentralised: there is no single supervisory authority — the Ministry of Justice plays only a coordinating role — and reports must be addressed to the competent authority for the relevant subject matter (Environmental Board for environmental violations, Financial Supervision Authority for the financial sector, Consumer Protection and Technical Regulatory Authority for product safety, etc.). Information about competent authorities is not compiled in a single accessible location, which the Estonian report explicitly identifies as a gap.

3.8 Identified legal gaps and ambiguities

Notwithstanding the broadly satisfactory formal alignment, the five reports identify a number of recurring gaps. (i) Aggregated national data: with the partial exception of Latvia (annual figures of approximately 386–409 reports, of which roughly one third recognised) and Italy (1,350 case files opened by ANAC in 2024), comprehensive national statistics are missing or under construction; both Romania and Estonia explicitly note the absence of an aggregated reporting system. (ii) Anonymous reports: Latvian law does not provide for the submission or examination of anonymous whistleblowing reports under the Whistleblowing Law (although KNAB accepts anonymous violation reports), while Polish law leaves the decision to the discretion of

Individual employers, with the result that the vast majority of public institutions surveyed refuse to process anonymous submissions on the merits. (iii) Material scope: the Estonian limitation to EU-law breaches is the most acute, but the Polish exclusion of labour-law violations from the mandatory catalogue is a similar source of dissatisfaction. (iv) Sanctions: Estonia, in particular, lacks penalties for failure to establish channels or to meet deadlines. (v) Support measures: free legal aid, psychological support and the involvement of civil society are everywhere weakly developed, with Italy and Latvia partial exceptions through, respectively, the third-sector register and Transparency International Latvia (Delna).

4. Organisation of Reporting Channels in Practice

4.1 Internal channels: roles, formalisation and written procedures

In all five countries, internal channels are by far the most frequently used and the most institutionally developed point of entry for whistleblowing. Their concrete configuration, however, varies. In Italy, internal channels are managed by the Anti-Corruption and Transparency Officer (RPCT) in public bodies, supported in larger institutions by dedicated units and working groups composed of staff with legal or investigative expertise; in some cases, particularly in non-profit organisations, the management of channels is entrusted to external independent bodies to strengthen perceptions of impartiality. In Romania, responsibility falls on a designated person or department, often drawn from the legal, internal control or audit areas, with formalised written procedures published on the institution's website. In Latvia, two officials are typically designated for whistleblowing matters, particularly in larger institutions, and operate under written procedures that are strictly followed. The Estonian model is similar but assigns the function predominantly to internal audit or internal control, given its perceived independence and direct line to top management. In Poland, the function rests on an internal reporting officer, often the internal auditor, with the law requiring the maintenance of a secure Internal Reporting Register.

Across the five countries, written procedures are the rule in larger institutions and the exception in smaller ones. The Estonian report notes that some smaller local governments rely on established practices and oral agreements rather than on a separate written document; the Italian and Latvian reports describe a comparable situation in small municipalities, where management of the channel is centralised in a single trusted figure (the general secretary in Italy; the head of internal audit in Latvia and Estonia).

4.2 Technological choices: digital, hybrid and analog solutions

Technology is the area where the five countries diverge most visibly. Italy stands out for the widespread use of dedicated digital platforms, in many cases based on open-source solutions developed by civil society (notably GlobaLeaks) or on internally developed applications. Most large central institutions and large municipalities have a digital platform that ensures confidentiality and traceable two-way communication, supplemented or replaced in smaller settings by certified email, in-person meetings and postal channels. Latvia exhibits a similar mix, with email as the primary internal channel, supported by web forms on institutional websites and intranets, dedicated phone lines, postal mail and even physical reporting boxes (although the latter struggle to escape the field of view of surveillance cameras in strategically important facilities). Estonia displays three groups of solutions: specialised external platforms in large organisations and international companies; web forms integrated into document management systems in the public sector; and simpler email/web-form solutions in smaller units.

Romania describes a system of dedicated email addresses, postal submission and direct reporting through scheduled meetings, with detailed procedures published on institutional websites. The most striking case is Poland, where the national report documents what it calls a “technological regression in the service of confidentiality”: in the public, local-government and academic sectors, decision-makers actively reject modern IT platforms because of their fear that internal IT departments could track logins and identify the senders of inconvenient reports. Importantly, this return to paper-based procedures is not portrayed as bureaucratic backwardness or a lack of digital capacity, but rather as a rationalised security choice — a form of physical “air gap” designed to eliminate digital traces such as IP addresses or server logs. The result is the emergence of analog channels — sealed envelopes, the “double envelope” system in city offices, traditional paper case files kept in physically secured rooms, and even the submission of correspondence in sealed envelopes that bypass the university’s main office and end up in a steel safe in the office of the responsible person. In close-knit public institutions, these mechanisms are perceived as the strongest guarantee of anonymity. By contrast, in the Polish private sector and in multinational corporations, digitalisation is widespread but generates a different problem — “procedural noise” caused by the coexistence of new statutory channels and long-standing global ethics hotlines, which leave employees uncertain about which tool to use to obtain statutory protection.4.3 External channels and the role of central or sectoral authorities.

Italy and Romania, as noted, rely on strong central authorities (ANAC and ANI). In both cases, the external channel is conceived as a backstop to internal channels, although the procedural relationship is somewhat tighter in Italy. Latvia’s recent transfer of the central contact point to KNAB consolidates expertise within an anti-corruption agency. Poland places the Ombudsman at the centre of the external system, alongside a network of sectoral ministries and inspectorates; the high volume of complaints reaching the Ombudsman’s office (around 690 in the first measurable period of 2025) reflects citizens’ trust in the institution but also the structural confusion between whistleblowing and ordinary administrative complaints under the Code of Administrative Procedure. Estonia’s decentralised model, where the whistleblower must independently identify the competent authority for the subject matter at stake, is the source of significant practical difficulties: information about the various competent authorities is not compiled in a single location, and the Ministry of Justice does not process individual cases or oversee implementation.

4.4 Cooperation with civil society, trade unions and external experts

Cooperation between obliged entities and external actors — civil society organisations, trade unions, independent experts, academic researchers — is weakly developed everywhere. The Latvian report describes interaction as “most commonly limited to consultations with KNAB or to the forwarding of cases to the competent authority”, with one notable exception: occasional cooperation with Transparency International Latvia (Delna), which provides legal support, advocacy and policy expertise and operates an online reporting portal (celtrauksmi.lv). In Italy, the third-sector register established by Legislative Decree 24/2023 provides a formal mechanism for support measures, although interviewees report that recourse to it remains rare. The Polish report highlights the role of trade unions in the financial sector and in clinical hospitals as quasi-monitors of the system, but notes that more structured cooperation is largely absent. Estonia and Romania describe minimal cooperation with NGOs, mostly limited to informal consultations.

4.5 Plurality and fragmentation of channels

A subtle but important issue, particularly visible in the Estonian and Polish reports, is the plurality of reporting channels. Many organisations operated existing channels — corruption hotlines, ethics complaints lines, adverse-event registries in hospitals, customer-complaint lines in regulated sectors — well before the transposition of the Directive, and have added the new statutory whistleblowing channel on top. The Estonian report describes one large municipality where a long-standing corruption hotline coexists with the new internal channel and, potentially, a third dedicated channel for personnel issues; the cumulative effect is that the role of the investigator becomes akin to “traffic control”. The Polish report describes a similar phenomenon in private corporations, where ethics hotlines and statutory channels overlap. The five reports converge on the conclusion that plurality is not in itself a flaw, but that it requires a clear central overview and clear communication to employees.

5. Reporting Practice: Volumes, Topics and Outcomes

5.1 Aggregated and institution-level data

The available quantitative picture is patchy and comparable only with caution. Latvia provides the most consistent national time series: between 2022 and 2024, the total number of whistleblowing reports remained relatively stable at around 386–409 per year, with approximately one third recognised as “well-founded whistleblowing reports” (111 in 2022, 106 in 2023 and 117 in 2024). Italy reports through ANAC: in 2024, ANAC opened 1,350 whistleblowing case files, of which 1,213 concerned reports of wrongdoing — predominantly from the public sector (970) compared to the private sector (243). After preliminary assessment, 388 cases were closed or deemed inadmissible, 263 declared inadmissible as manifestly unfounded, 277 referred to other competent authorities, and 285 considered admissible for further investigation.

Romania publishes data only on the external channel managed by ANI: 47 reports in 2023 and 99 in 2024 (83 nominal, 16 anonymous) — a low volume relative to the size of the public administration. At the institutional level, the Romanian report shows striking unevenness: the Ministry of Environment registered 1 report in 2023, 5 in 2024, 34 in 2025 and 4 in early 2026; the City Hall of Timișoara recorded 45 reports in two years (none confirmed); the City Hall of Sector 1 in Bucharest registered only two reports; many county councils, large municipalities (Cluj-Napoca, Oradea) and universities (Babeș-Bolyai, UMF Iași, UMF "Carol Davila") recorded zero reports.

Poland reports the most striking statistical picture. Most surveyed central agencies, ministries, universities, multi-specialty hospitals and municipal offices recorded zero formally compliant reports during the first months of the law’s operation. The only systemic exception is the Ombudsman’s office, which received nearly 690 cases in the first measurable period of 2025; only 32% of them (223 cases) met the formal substantive requirements of the new law. Estonia, finally, has no national aggregated data: the available picture is built up from institutional self-reporting, with usage that varies from zero to a few dozen per year depending on the institution; in larger organisations, only 10–20% of submissions qualify as serious legal violations, corruption, fraud or work-related misconduct.

5.2 Public vs private sector trends

In Italy, ANAC data show a clear predominance of reports from the public sector (970 vs. 243 in 2024), suggesting both higher exposure and higher visibility of the channel in public bodies. In Latvia, the public-sector dominance is similar, although well-functioning systems also exist in some state-owned and private companies; reports from the private sector remain comparatively sparse, and the national report explicitly attributes the low responsiveness of private companies during interview recruitment to the absence of internal channels and to insufficient information about whistleblowing mechanisms. Poland’s private sector is dominated by multinational corporations whose pre-existing global compliance frameworks predate the new statutory channels;

the Polish report describes those organisations as "islands of hope" that progressively de-stigmatise reporting through Western compliance culture. Romania and Estonia present a comparable mix.

5.3 Typology of reports: corruption, integrity, HR/interpersonal issues, "noise"

A finding common to all five reports — and arguably the single most important practical observation of this comparative analysis — is that whistleblowing channels are not used predominantly to surface integrity violations. In Italy, interviews show that reports rarely concern corruption in the strict sense; the bulk relates to employment-related issues, interpersonal conflicts, internal organisational matters or the misuse of the channel for personal purposes. In some contexts — particularly large central institutions — the system is used strategically to anticipate or counter disciplinary proceedings or for retaliatory purposes, a distortion noted in several Italian interviews. In Latvia, the most common topics are public procurement irregularities, conflicts of interest, misuse of EU funds, mobbing/bossing, labour rights and sector-specific issues (healthcare and construction). In Estonia, interviewees explicitly distinguish three categories: rare "classic" legal breaches; a predominant set of HR and interpersonal issues; and significant "noise" (technical failures, unrelated complaints, even reports of broken light bulbs). Estonian respondents estimate that 80–90% of submissions do not relate to serious legal violations.

In Poland, the dominant pattern is what the report calls "definitional chaos": citizens systematically confuse the whistleblowing procedure with ordinary complaints and petitions filed under the Code of Administrative Procedure, and within healthcare there is recurrent confusion with the safe Adverse Event Registry (RZN). At the institutional level studied, no single valid report compliant with the Act was physically submitted during the initial period; ministry employees contacted the coordinator only to ask for clarifications about the law. Romania presents a similar profile: at the central administration level, reports tend to reflect classic integrity areas (public procurement, conflicts of interest, use of public/EU funds, internal management); at the local level, where reports exist they mostly concern administrative dysfunctions; in the academic environment, reporting is almost absent.

5.4 Procedural duration and outcomes

The seven-day acknowledgement is generally respected across the five countries. The three-month feedback deadline is also broadly met, although practice diverges in two directions. In some institutions — particularly large Italian municipalities — processing is significantly faster (sometimes under one month), often because reports are closed at an early stage without complex investigations. The Latvian report cites an average handling time of approximately 3.5 months, with smaller institutions deciding on recognition within three to four days, and resolution sometimes extending to over a year for complex cases. The Estonian report notes feedback typically within 30 days to three months for non-anonymous reports, with anonymous reports limited by the technical capabilities of the channel.

Outcomes converge across the five countries on a striking finding: substantiated cases are extremely rare. The Italian report describes “a near-total absence of reports confirmed as substantiated”, raising questions about the system’s actual capacity to detect significant instances of corruption or maladministration. The Latvian report indicates that recognised reports most commonly lead to organisational improvements rather than purely punitive outcomes — reviews of internal procedures, internal audits, mediation in interpersonal cases — with disciplinary measures being rare. The Estonian report makes the same point and notes that disciplinary actions, when imposed, typically result from information obtained through sources other than the official whistleblowing channel.

5.5 The “underuse” phenomenon: deafening silence and definitional chaos

The cumulative picture from the five reports is that of an architecture that is technically in place but rarely fully activated. The Polish report captures this with the phrase “deafening silence”: the statistical void of internal channels is not, the report argues, evidence of an absence of misconduct in Polish public life, but the result of definitional chaos, lack of legal awareness and — most importantly — fear of consequences. Romania, Italy, Latvia and Estonia describe the same phenomenon in less dramatic terms: many institutions, particularly smaller ones, record zero reports, while in those that do receive reports, the bulk does not concern the integrity violations that the Directive was designed to surface. The implication is that the question for the years ahead is less whether national systems are formally compliant, and more whether they will be able to evolve from formal compliance to substantive use.

6. Whistleblower Protection in Practice

6.1 Confidentiality as the cornerstone of protection

All five national reports converge on the observation that confidentiality is, in practice, the primary and often the only effective protection mechanism. The technical safeguards are largely the same: pseudonymisation of personal data, restricted access to the report and to the related materials, separate registers, audit trails of access, encryption of communications and (where used) secure platforms with two-way communication via alphanumeric codes. The Italian and Estonian reports emphasise the role of dedicated digital platforms in keeping access narrow; the Latvian report notes that recognised reports are stored in a separate system from the general document management system, with access limited to designated contact persons and (in some cases) ethics-commission members; the Romanian report describes the use of separate registers, access restrictions and pseudonymisation as standard institutional practice. The Polish report describes both very advanced and very rudimentary set-ups, depending on the sector.

Practical limitations are also recognised everywhere. In small municipalities, in academic departments and in healthcare units with stable staff and tight social networks, the content of a report — even when stripped of identifying information — may allow indirect inference of the whistleblower's identity. The Estonian report describes the use of "masking" techniques (verifying information during a routine audit or planned inspection) precisely to break the link between the report and the inquiry; the Italian report acknowledges that, in smaller organisations, despite formal protection mechanisms, the possibility of indirectly identifying the whistleblower remains high.

6.2 Treatment of anonymous reports

The handling of anonymous reports is the area where the five countries diverge most sharply, and the divergence is not merely theoretical: it shapes the practical accessibility of the system. Latvian law does not provide for the submission or examination of anonymous whistleblowing reports under the Whistleblowing Law, although KNAB accepts anonymous "violation reports" outside that framework, with the submitter receiving an identification number and an access password to follow the case. The Latvian report identifies this as a clear shortcoming, particularly in a small country where social and professional networks are tight, and notes that interviewees repeatedly emphasised the importance of anonymous reporting.

Polish law leaves the decision on anonymous reports to individual employers. The Polish report shows that the vast majority of public institutions and clinical hospitals refuse to consider anonymous reports on the merits, justifying the position by the desire to protect team stability from "anonymous notes tossed into boxes due to personal conflicts"; central authorities (the Ombudsman, ministries) take a more conditional approach, processing unsigned cases when they are supported by objective and credible evidence. Italian, Romanian and Estonian frameworks accept anonymous reports, with operational caveats: the Italian report describes a "tension between the need to guarantee anonymity and the requirement to obtain sufficiently detailed information", with anonymous reports processed only if substantively complete; the Romanian system formally permits anonymous reports through ANI but limits the protection by precluding further communication; the Estonian system accepts anonymous reports but their processing depends on the technical capacity of the channel for two-way communication.

6.3 Retaliation prevention and monitoring measures in practice

The reports paint a remarkably consistent picture of retaliation prevention and monitoring as the weakest link of the protection architecture. None of the five countries operates structured monitoring systems for retaliation. The Italian, Estonian and Latvian reports note the absence of dedicated units, specific protocols or systematic measures to support whistleblowers in the post-reporting phase. The Polish report describes a strategy of "passive monitoring": even ombudsmen serving in central government bodies admit they have virtually no managerial tools within the institution to combat ongoing retaliation beyond formally reporting the conduct to law-enforcement agencies. The Romanian report similarly notes the absence of a consolidated public system for monitoring retaliation at the national level.

Documented cases of retaliation are scarce. In all five reports, interviewees and institutions stated that they had not encountered direct, clearly identifiable cases of retaliation; in all five reports, however, the authors caution that the absence of cases cannot be read as the absence of the phenomenon, given the low number of reports overall, the difficulty of documenting subtle forms of retaliation (marginalisation, reassignment of duties, denial of training, reputational damage), and the absence of systematic follow-up. The Latvian report cites a particularly telling indicator: in one municipality, a responsible person reported repeated inquiries from senior representatives about whether reports had been submitted and by whom, raising concerns that retaliation could occur if a whistleblower were identified.

6.4 Support measures: legal aid, psychological support, civil society involvement

Support measures are everywhere underdeveloped. The Italian Decree provides for support measures through third-sector entities listed in a dedicated register — free information, assistance and advice on reporting procedures, protection against retaliation, the rights of the persons involved and access to legal aid — but interviews report that recourse to these measures remains limited; psychological support, where offered, is generally part of services already provided to staff, and the role of the RPCT often becomes that of an informal point of contact for the whistleblower throughout the procedure. Romania relies on counselling, guides and information materials provided by ANI, complemented by training sessions and methodological tools developed within the SNA framework. Latvia operates through the State Labour Inspectorate (consultations on remedies in employment relationships and occupational safety), trade unions and Transparency International Latvia (Delna); the most visible form of support, however, remains legal consultation provided by the responsible persons themselves, who are often legal professionals.

Estonia describes the absence of free legal aid for whistleblowers and the reliance on general HR benefits, including psychological support through occupational health services; the role of the case handler as a “trusted listener” is highlighted as an important informal support, particularly in emotionally complex situations. Poland is the most critical case: organisations enjoy complete discretion in providing institutional support (psychological or legal), and the structural inefficiency of Polish labour courts makes the formally available judicial remedy effectively unavailable.

6.5 Effectiveness of judicial remedies

The reversal of the burden of proof exists in all five jurisdictions. Its effectiveness, however, depends on the practical accessibility of judicial remedies. The Polish report describes this aspect with particular force: although the law shifts the burden of proof onto the employer, the prospect of a labour-court case lasting three to five years across all instances, during which a dismissed and stigmatised whistleblower is left without means of support, “effectively and ruthlessly paralyses decisions to disclose even the most obvious abuses”. The data of the National Labour Inspectorate confirm the social fear of the courts: out of approximately 50,000 employee complaints registered annually, only a dozen or so concern retaliatory actions against whistleblowers, of which only one was deemed fully justified after investigation. The other four reports do not raise comparable concerns about the formal functioning of courts, but the Italian and Latvian reports note that interviewees expressed doubts about the actual effectiveness of protection mechanisms, and the Estonian and Romanian reports note that the reliance on individual case handlers’ judgement makes effective protection contingent on personal attentiveness rather than on a coherent system.

7. Cross-cutting Challenges and Strengths

7.1 Cultural barriers and the "snitch" stigma

The single most pervasive obstacle identified across the five reports is cultural. The Polish report devotes its longest section to the "invisible historical-sociological culture of silence" that equates an honest person reporting irregularities with a "snitch", an "informer" or even a traitor — a stigma rooted in 123 years of foreign occupation and decades of post-1945 communist authoritarianism, and still actively transmitted in mocking comments during onboarding training. The report also highlights a marked generational divide: younger employees often approach whistleblowing with pragmatic detachment, preferring to resign and seek employment elsewhere rather than engage in lengthy reporting procedures, while older employees tend to be constrained by economic self-calculation and fear of retaliation. The Estonian report describes a comparable pattern: the historical association of reporting breaches with negative "snitching" persists, particularly among older generations and in certain institutions, even though younger employees increasingly view whistleblowing as a normal part of organisational culture. The Latvian report stresses the "cultural stigma and prejudice against reporting" deeply embedded in many organisations, and the importance of shifting the perception of whistleblowing from an act of disloyalty to a responsible measure that contributes to organisational improvement. The Italian report identifies, in addition, a tendency to rely on informal or hierarchical channels (direct supervisors, human-resources departments) rather than formal whistleblowing mechanisms — a pattern that may signal trust in traditional internal processes but undermines traceability and the standardisation of reporting practice. Romania, finally, describes a low level of trust in protection mechanisms and a "predominantly formal" implementation, which together depress the use of channels.

At the same time, the reports indirectly highlight a broader unresolved issue in European whistleblowing frameworks: while none of the analysed systems provides financial incentives comparable to those found in some Anglo-Saxon jurisdictions, the introduction of such mechanisms could itself prove culturally controversial, potentially reinforcing perceptions of whistleblowers as opportunistic or disloyal actors rather than individuals acting in the public interest.

7.2 Trust, institutional memory and post-transition legacies

The legacy of authoritarian or transitional histories — explicitly invoked in Poland, more discreetly present in Romania and the two Baltic countries — has lasting institutional consequences. In Poland, distrust of internal IT departments drives the technological regression toward analog channels; in small communities, the "ironclad rule that everyone in town knows everyone else" turns the legal guarantee of anonymity into what one Polish interviewee called "a legal fiction and a pipe dream". More broadly, the reports show that in close-knit local environments the exposure of a whistleblower may carry consequences extending well beyond the workplace, including long-term professional exclusion and social ostracism affecting not only the individual but also their family network. In Romania, the report notes that monitoring relies on the National Anti-Corruption Strategy, but its findings show that mechanisms "are more formally implemented than actually used". In Latvia, interviewees emphasise the difficulty of building employee confidence in close-knit institutions where the content of a report can betray its source. The Italian report adds an organisational dimension: in non-profit organisations and in small municipalities, the centralisation of multiple functions in single individuals (the general secretary, the RPCT) creates structural risks of indirect identification.

Across several contexts, moreover, public perceptions of whistleblowing are shaped not only by organisational culture but also by media narratives: highly publicised cases of retaliation, disciplinary sanctions or institutional conflict may inadvertently reinforce distrust in protection mechanisms and generate a broader chilling effect on potential reporters.

7.3 The implementation gap: from formal compliance to effective use

The most concise way to summarise the cumulative picture is the gap between formal compliance and effective use. All five countries have transposed the Directive in formally compliant terms and have set up the architecture it requires. All five also describe a shared set of practical shortcomings: low and uneven volumes of reports, predominance of HR/interpersonal issues over integrity violations, near-absence of substantiated cases, limited and informal support, weak retaliation monitoring and weak civil-society involvement. The implementation gap is widest in Poland and Estonia, where the systems are youngest; it persists in Romania, where the legal framework has been in place since 2022; and it is significant even in Italy and Latvia, where the systems are most mature. This suggests that the gap is not primarily a function of time, but of structural and cultural factors that the law alone cannot address.

7.4 Emerging good practices

Against this backdrop, the five reports identify a number of emerging good practices that deserve to be highlighted and disseminated. In Italy, the use of open-source digital platforms (GlobaLeaks) and the integration of whistleblowing into broader compliance frameworks (Organisational and Management Models under Legislative Decree 231/2001 in the private sector and Integrated Plans of Activities and Organisation, PIAO, in the public sector) embed reporting within wider risk-prevention systems. In Latvia, good practice includes assigning a limited number of personnel to handle whistleblowing matters, ensuring strict anonymity of the whistleblower, applying the four-eyes principle, preparing centralised statistics and an annual report on cases, and including representatives from different professional fields on ethics committees. In Estonia, the "masking" of investigations within routine audits, the use of secure platforms supporting anonymous two-way communication, and the role of clear value-based messaging from top management have been identified as the most effective practices. In Poland, despite the difficult overall picture, the report identifies the "two-channel system" in small municipalities (a trusted HR employee verifies employment status without seeing the substance, and the substance is then handled by an independent auditor working with anonymised material), the hybrid classification system in clinical hospitals, the use of regular intranet “reminders”, and the role of multinational corporations in slowly de-stigmatising reporting through Western compliance culture. Romania highlights the combined value of clear public written procedures, multiple reporting channels, the explicit designation of responsible persons and the centralised role of ANI in coordinating the system.

8. Comparative Synthesis

8.1 Key convergences across the five countries

Five major convergences emerge from the analysis. First, the formal alignment with Directive 2019/1937 is strong across all five jurisdictions: scope, channels, deadlines, confidentiality, prohibition of retaliation and reversal of the burden of proof are present everywhere. Second, the implementation gap is universal: low volumes of reports, predominance of non-integrity issues, near-absence of substantiated cases, weak retaliation monitoring. Third, confidentiality dominates the protective architecture in practice, while structured retaliation prevention and support measures remain marginal. Fourth, cultural barriers — the "snitch" stigma in Poland, Estonia and Romania, organisational closure and the preference for informal channels in Italy and Latvia — are the single most consistently cited obstacle. Fifth, civil society and trade unions are weakly integrated in all five frameworks, with the partial exceptions of Italy (third-sector register) and Latvia (Delna).

8.2 Key divergences and country-specific features

Three significant divergences stand out. The first is the institutional architecture of external oversight: centralised and powerful in Italy (ANAC) and Romania (ANI), recently consolidated within KNAB in Latvia, distributed between the Ombudsman and sectoral inspectorates in Poland, and explicitly fragmented and decentralised in Estonia. The second is the treatment of anonymous reports: are not accepted and processed under the Whistleblowing Law in Latvia (with KNAB providing an anonymous "violation report" track outside that framework), discouraged in practice in Poland through employer discretion, and conditionally accepted in Italy, Romania and Estonia. The third is the material scope: broad in Italy, Romania, Latvia and Poland (with the explicit Polish exclusion of labour law from the mandatory catalogue), and deliberately narrow in Estonia, where protection covers only breaches of EU law.

Each country also exhibits at least one defining feature. Italy has the most articulated central authority (ANAC) and the most widespread use of digital platforms, paired with a clear preference for internal channels. Romania combines a strong ANI-centred external framework with very limited use at the local and academic level. Latvia is the longest-running system in the group, anonymous whistleblowing reports are not accepted and a recent (2026) consolidation under KNAB. Poland is the most acute case of the implementation gap, with "deafening silence" in internal channels, "technological regression" toward analog tools and a structural problem with the labour courts. Estonia is the most decentralised model and the only one with a scope explicitly limited to EU-law breaches.

8.3 Country snapshots

Italy

Legislative Decree 24/2023 transposes the Directive horizontally, repealing previous fragmented regimes (Article 54-bis of Legislative Decree 165/2001 and Law 179/2017). The system rests on a clear preference for internal channels, with ANAC operating the external channel and exercising supervisory and sanctioning powers. Reporting channels are typically digital, often based on open-source GlobaLeaks software. Protection is centred on confidentiality and on the broad prohibition of retaliation, with the reversal of the burden of proof. The persistent challenge is the low volume of reports, the predominance of HR/interpersonal submissions, the near-absence of substantiated cases and the rudimentary state of retaliation monitoring and support measures. The integration of whistleblowing into broader compliance frameworks (Legislative Decree 231/2001; PIAO) is a systemic strength.

Romania

Law 361/2022 transposes the Directive after a partial earlier framework (Law 571/2004) limited to the public sector. The architecture relies on a strong central authority (ANI) and on the National Anti-Corruption Strategy 2021–2025. Reporting volumes are very low (47 external reports in 2023, 99 in 2024) and unevenly distributed: many county councils, large city halls (Cluj-Napoca, Oradea) and universities (Babeș-Bolyai, UMF Iași, UMF "Carol Davila") record zero reports, while a few institutions (Ministry of Environment, City Hall of Timișoara) record significant volumes. The legal framework provides solid guarantees, but practical use lags behind, particularly at the local and academic levels. The main challenge is the transition from formal compliance to effective use.

Estonia

The Act on Protection of Persons Who Report Work-Related Breaches of European Union Law entered into force on 1 September 2024. The personal scope is broad, but the material scope is deliberately limited to EU-law breaches, leaving many domestic concerns outside protection. Oversight is fragmented and decentralised, with no single supervisory authority. Internal channels are managed primarily by internal audit. Confidentiality is the cornerstone of protection, supported in larger organisations by external platforms with two-way anonymous communication. Reports are dominated by HR and interpersonal issues; substantive integrity violations are rare. Cultural stigma toward “snitching” persists, particularly in older generations. The system is in place but not yet fully developed; clearer guidance, broader scope and better support are required.

Latvia

The 2018 Whistleblowing Law, replaced by the 2022 Law and amended on 1 March 2026, is the longest-running framework in the group. The scope of protection is among the broadest in the EU. The 2026 amendments transferred the central contact point to KNAB, expanded the definition of “associated person” to facilitators and supporting legal entities, and introduced specific liability for unlawful disclosure. Internal channels (especially dedicated email) dominate; external reporting is secondary. The most distinctive feature is the anonymous whistleblowing reports are not accepted under the Whistleblowing Law (although KNAB accepts anonymous violation reports). Volumes of reports are stable (around 386–409 per year, of which roughly one third recognised as well-founded), with a similar predominance of HR and procurement issues. Civil society (notably Delna) plays a more visible support role than in the other four countries.

Poland

The Act of 14 June 2024, adopted nearly three years late and under EU financial pressure, is described by the Polish national report as a “highly technocratic” framework. The first measurable period of 2025 reveals a phenomenon of “deafening silence”: most institutions surveyed recorded zero formally compliant internal reports. The Ombudsman’s office serves as the central external authority, receiving nearly 690 cases (32% recognised as substantive) in the first measurable period. Striking features include the “technological regression” of public, local-government and academic sectors toward analog channels (sealed envelopes, double-envelope systems, paper case files in physical safes), the practice of refusing anonymous reports in most public bodies, the structural inefficiency of labour courts undermining the reversal of the burden of proof, and the deeply rooted cultural stigma equating whistleblowers with “snitches” or informers. The report calls for systemic revision before the law becomes “a dead letter”.

9. Policy Recommendations

The recommendations below are organised by addressee. They are derived from the cumulative findings of the five national reports and aim at closing the implementation gap that the comparative analysis has documented.

9.1 For EU institutions

First, the European Commission should consider issuing supplementary guidance or a recommendation on the substantive examination of credible anonymous reports, addressing the wide variation in national practice (from the Latvian prohibition to the Polish employer discretion). Second, EU monitoring of transposition should evolve from formal compliance checks toward structured indicators of practical implementation: aggregated reporting volumes, share of substantiated reports, time to feedback, documented retaliation cases and judicial outcomes. Third, the Commission should support cross-country exchanges between national competent authorities (ANAC, ANI, KNAB, the Polish Ombudsman, the Estonian Ministry of Justice and the relevant Estonian sectoral authorities), including secondments, joint trainings and shared anonymised case studies. Fourth, EU funding should be made available for national de-stigmatisation campaigns and for the development of secure, open-source reporting platforms in line with Italian best practice (GlobaLeaks).

9.2 For Member States

First, Member States should clarify the legal status of anonymous reports, ideally by requiring the substantive examination of credible, evidence-supported anonymous reports — in line with the recommendation issued by the Polish national report. Second, Member States with narrow scope (notably Estonia) should consider broadening protection to cover key domestic concerns (theft, fraud, conflicts of interest in non-EU areas, workplace violence). Third, Member States should designate a single point of information that lists, in a clear and accessible form, all competent authorities for external reporting (a particularly acute need in Estonia). Fourth, Member States should invest in retaliation monitoring: dedicated central or sectoral structures, follow-up duties on competent authorities, and aggregated annual reports. Fifth, Member States should consider providing free legal aid and structured psychological support to whistleblowers — services that, today, are nominally available only in some jurisdictions (Italy, partially Latvia) and absent or discretionary elsewhere.
Specifically, Poland should consider revising the Act of June 2024 to (i) require the substantive examination of credible anonymous reports, (ii) include broadly defined labour law in the mandatory catalogue, (iii) launch a state-sponsored awareness and de-stigmatisation campaign, (iv) reform labour-court procedures to reduce the average duration of retaliation cases. Romania should accelerate the development of a national aggregated reporting system and invest in institutional capacity at the local and academic levels. Italy should strengthen support measures for whistleblowers and develop systematic retaliation monitoring beyond the confidentiality-based

architecture. Latvia should reconsider the prohibition on anonymous whistleblowing reports under the Whistleblowing Law, in light of the small size of the country and the fragility of anonymity in close-knit communities. Estonia should designate a single supervisory authority, broaden the scope of the Act to cover key domestic concerns, and establish clear rights to interim relief and full compensation for damages.

9.3 For obliged entities (public administration and employers)

First, obliged entities should formalise written procedures, even in small organisations, and ensure that they are publicly accessible and clearly distinct from ordinary administrative-complaint channels. Second, they should invest in training and awareness for all staff, with particular attention to the distinction between whistleblowing and ordinary HR or grievance channels. Third, they should designate at least two responsible persons (the four-eyes principle is widely cited as good practice in Latvia and Estonia) and avoid concentrating multiple sensitive functions in a single individual. Fourth, where the size of the organisation allows, they should adopt secure platforms with two-way anonymous communication, ideally based on audited open-source software. Fifth, they should develop a clear policy on anonymous reports that ensures, at a minimum, the substantive examination of credible, evidence-supported submissions. Sixth, they should take active responsibility for retaliation monitoring, with periodic check-ins with the reporting person after the conclusion of the procedure.

9.4 For civil society and supporting actors

Civil society organisations and trade unions are weakly integrated in the whistleblowing architecture of all five countries. This creates space for a more proactive role. First, they should expand the offer of free legal advice and psychological support, building on the model of Transparency International Latvia (Delna) and on the third-sector register established in Italy. Second, they should run advocacy campaigns to address the “snitch” stigma, particularly in countries with strong post-transition legacies (Poland, Romania, Estonia). Third, they should systematically collect and publish anonymised case studies and statistics, partly compensating for the patchy aggregated data provided by national authorities. Fourth, they should engage with national competent authorities in structured fora — combining the German tradition of sectoral compliance dialogues, the French Médiateur tradition and the Anglo-Saxon practice of guidance through anonymised case studies. Fifth, they should advocate at the EU level for the systematic inclusion of practical-implementation indicators in the Commission’s monitoring of the Directive.

10. Conclusion

Five years after the entry into force of Directive (EU) 2019/1937, the formal alignment of national whistleblowing systems with the European standard is largely satisfactory across the five Member States covered by this report. Italy, Romania, Latvia, Estonia and Poland have all transposed the Directive in formally compliant terms; all five have set up internal and external reporting channels, designated responsible persons and competent authorities, codified the seven-day acknowledgement and three-month feedback deadlines, prohibited retaliation in broad terms and embedded the reversal of the burden of proof in their national legislation. Where they differ — anonymous reports in Latvia, scope in Estonia, the centralised authority architecture in Italy and Romania, the technological regression in Poland — they do so within a framework that meets, and in some cases exceeds, the Directive's minimum standards.

The picture changes when the analysis turns to practice. The five reports converge on a single diagnosis: a substantial implementation gap separates the formal architecture from its effective use. Volumes of reports are low and unevenly distributed, the typology is dominated by HR and interpersonal matters rather than integrity violations, substantiated cases are rare, retaliation monitoring is largely absent, support measures are underdeveloped, and cultural barriers — the "snitch" stigma in countries with post-transition legacies, the preference for informal hierarchical channels in others — are the single most pervasive obstacle. The implementation gap is wider in countries where the system is most recent (Poland, Estonia), but it persists also where the framework is older (Italy, Latvia, Romania), suggesting that time alone will not close it.

Closing the gap will therefore require deliberate action at all four levels addressed by the recommendations: the EU institutions setting the standard and monitoring its practical implementation; Member States adapting their legal frameworks and investing in awareness, training and support; obliged entities formalising procedures and embedding whistleblowing into their organisational culture; civil society and trade unions expanding their advocacy and support role. The cumulative finding of the five reports — that the legal text is necessary but not sufficient — is a familiar one in EU policy implementation. The specificity of whistleblowing is that the asymmetry between the formal and the substantive is particularly acute, because the system relies on the courage and trust of individual citizens. Without that trust, no procedure, however well designed, will deliver on the promise of the Directive.

Co-funded by the European Union. Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by
the European Union