Co-funded by the European Union

Whistleblower Empowerment & Support Initiative

Best Practices Research Report & Toolkit

VoiceGuard project

FIBGAR NOVEL Group TRANSPARENCY INTERNATIONAL BULGARIA oživení TRANSPARENCY INTERNATIONAL ROMANIA md_brainnovation

DISCLAIMER
Funded by the European Union. Views and opinions expressed in this Deliverable are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for the content.

STATEMENT OF ORIGINALITY: This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both.

COPYRIGHT: This work is licensed by the CEBCAT Consortium under a Creative Commons Attribution-ShareAlike 4.0 International License, 2023. For details, see http://creativecommons.org/licenses/by-sa/4.0/

CERV-2024-CHAR-LITI-WHISTLE
GRANT AGREEMENT NUMBER: 101213588

Contents

1. Executive summary ... 3
2. Introduction ... 11
2.1 Context and Conceptual Framework ... 11
2.2 Conceptual framework ... 13
3. International and European Standards ... 16
3.1 The EU Whistleblowing Directive (EU) 2019/1937 ... 16
3.2 Council of Europe Recommendation CM/Rec (2014)7 ... 17
3.3. United Nations Convention against Corruption (UNCAC) ... 18
3.4. OECD best practice ... 18
4. Methodology and Analytical Approach ... 20
4.1. Research Design and Data Collection Framework ... 20
4.2. Data collection ... 20
4.3. Data Analysis Approach ... 21
4.4. Data Quality and Limitations ... 22
5. Core Pillars of Effective Whistleblowing Protection ... 23
5.1. Normative Foundations ... 23
5.2. Reporting Channels and Accessibility ... 25
5.3. Institutional Design and Independence ... 28
5.4. Protection Measures and Support Mechanisms ... 29
6. Implementation, Culture and Effectiveness ... 31
6.1. Training, Awareness and Organizational Culture ... 31
6.2. Monitoring, Evaluation and Continuous Improvement ... 31
7. Conclusions ... 33
8. Annexes ... 38
8.1. Annex 1. Toolkit for Whistleblower Protection ... 38
8.2. Annex 2. Questionnaire on good practices in the transposition and implementation of the EU Directive 2019/1937 on the protection of persons who report breaches of Union law ("the Whistleblowing Directive") ... 40
8.3. References ... 42

1. Executive summary

From diagnosis to possible solutions

The *Good Practice Report* forms part of the VoiceGuard: Whistleblower Empowerment & Support Initiative, implemented under the Citizens, Equality, Rights and Values (CERV) Programme. It constitutes Deliverable 2.3 within Work Package 2 and builds directly on the empirical findings of the Needs Analysis and Skills Assessment previously conducted within the project.

The starting point of this report is a central paradox identified in the Needs Analysis: although Directive (EU) 2019/1937 established a harmonised minimum standard of whistleblower protection across the European Union, lived experiences of whistleblowers frequently remain characterised by retaliation, procedural hostility, institutional silence, and prolonged litigation.

Formal legal transposition does not automatically translate into effective protection. Reporting channels may exist, but trust in them remains fragile. Anti-retaliation provisions may be codified, yet reprisals continue in more subtle or strategic forms. Judicial remedies may ultimately be available, but only after years of professional and personal harm.

The Good Practice Report responds to this gap between "paper protection" and substantive protection. Its purpose is not to restate minimum legal standards, but to identify operational, institutional, procedural and cultural arrangements that demonstrably strengthen whistleblower protection in practice.

Methodological approach

The report applies a qualitative and comparative methodology. It integrates:

- Findings from 16 in-depth whistleblower interviews and 32 expert consultations conducted in six EU Member States;
- Structured questionnaire responses from project partners and Transparency International chapters;
- Comparative legal analysis against Directive (EU) 2019/1937, OECD best practice standards, Council of Europe Recommendation CM/Rec (2014)7, and relevant international instruments.

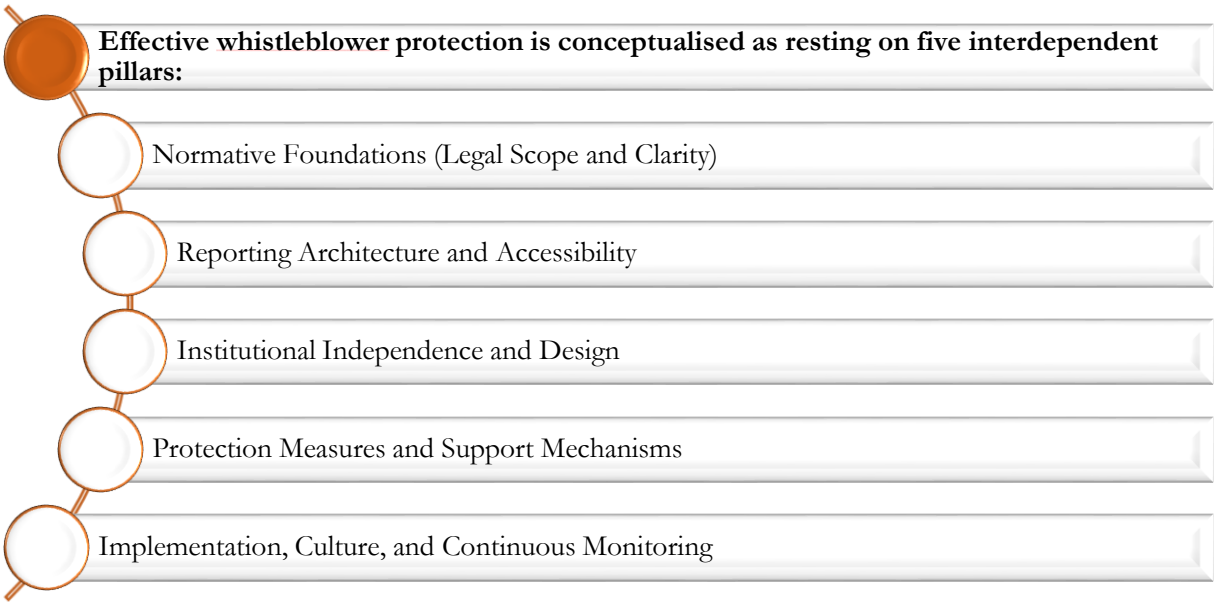
Rather than offering a statistically representative survey of all Member States, the report identifies transferable good practices through problem–solution mapping. Practices were assessed not only for normative alignment but for their responsiveness to empirically documented shortcomings.

Conceptual framework: five interdependent pillars

Effective whistleblower protection is conceptualised as resting on five interdependent pillars:

i. Normative Foundations (Legal Scope and Clarity)
ii. Reporting Architecture and Accessibility
iii. Institutional Independence and Design
iv. Protection Measures and Support Mechanisms
v. Implementation, Culture, and Continuous Monitoring

Weakness in any pillar undermines system credibility and effectiveness.



Normative foundations: breadth and legal certainty

A key finding is that broad and clear legal scope enhances both legitimacy and accessibility. Good practices identified include:

- Extending material scope beyond EU-law breaches to include violations of national law and public interest wrongdoing;
- Broad personal scope covering employees, former employees, contractors, trainees, facilitators and related persons;
- Explicit protection of facilitators and third parties vulnerable to retaliation;
- Operationalisation of the "reasonable belief" standard, ensuring protection does not depend on ultimate confirmation of wrongdoing.

Good practices identified include:

- Extending material scope beyond EU-law breaches to include violations of national law and public interest wrongdoing
- Broad personal scope covering employees, former employees, contractors, trainees, facilitators and related persons
- Explicit protection of facilitators and third parties vulnerable to retaliation
- Operationalisation of the "reasonable belief" standard, ensuring protection does not depend on ultimate confirmation of wrongdoing.

Particularly impactful form the perspective of the legal framework is the reversal of the burden of proof in retaliation cases. Where detriment follows a protected disclosure, the employer must demonstrate that the measure was unrelated to reporting. This reduces evidentiary barriers and creates meaningful deterrence.

Reporting architecture: accessibility, trust and security

The existence of reporting channels is insufficient; their credibility determines usage.

Effective systems demonstrate:

- Multi-channel reporting (digital, telephone, in-person);
- Secure digital platforms enabling anonymous two-way communication;
- Clear timelines for acknowledgment and feedback;
- Structured intake and early risk assessment;
- Transparent escalation pathways for cases involving senior leadership;
- Publicly accessible guidance in plain language.

Effective systems demonstrate:

- Multi-channel reporting (digital, telephone, in-person);
- Secure digital platforms enabling anonymous two-way communication;
- Clear timelines for acknowledgment and feedback;
- Structured intake and early risk assessment;
- Transparent escalation pathways for cases involving senior leadership;
- Publicly accessible guidance in plain language.

Anonymity and confidentiality must be technically credible. Systems must prevent metadata leakage, limit access, and ensure secure handling. Where whistleblowers distrust internal channels, accessible and independent external authorities are essential.

Public disclosure provisions must remain realistic and clear. Overly restrictive escalation rules risk deterring reporting precisely when internal and external channels fail.

Institutional independence: credibility as a determinant of reporting

Institutional design strongly shapes whistleblower behaviour. Good practice includes:

- Independent external authorities with investigative powers;
- Budgetary and functional autonomy;
- Transparent appointment processes;
- Fixed-term leadership with protected tenure;
- Clear mandates and conflict-of-interest safeguards;
- Oversight mechanisms balancing independence and accountability.

Institutional design strongly shapes whistleblower behaviour. Good practice includes:

- Independent external authorities with investigative powers
- Budgetary and functional autonomy
- Transparent appointment processes
- Fixed-term leadership with protected tenure
- Clear mandates and conflict-of-interest safeguards
- Oversight mechanisms balancing independence and accountability

Special arrangements for handling reports implicating senior leadership are particularly important. Predefined escalation routes to independent bodies prevent conflicts of interest and reinforce trust.

Protection measures: from reactive to preventive systems

A central conceptual shift identified in strong frameworks is movement from reactive to preventive protection.

Traditional systems rely heavily on ex post remedies (litigation and compensation). However, retaliation often unfolds rapidly, while judicial proceedings are slow. This temporal mismatch creates structural vulnerability.

High-impact preventive practices include:

- Interim relief preventing dismissal or disciplinary action;
- Presumption of retaliation when detriment follows reporting;
- Nullity of retaliatory acts;
- Administrative fines for retaliators;
- Early-stage risk assessment;
- Access to legal aid and public defenders;
- Transparent disciplinary procedures;
- Psychological support mechanisms;
- Temporary financial assistance in cases of severe deterioration.

High-impact preventive practices include:

- Interim relief preventing dismissal or disciplinary action
- Presumption of retaliation when detriment follows reporting
- Nullity of retaliatory acts
- Administrative fines for retaliators
- Early-stage risk assessment
- Access to legal aid and public defenders
- Transparent disciplinary procedures
- Psychological support mechanisms
- Temporary financial assistance in cases of severe deterioration

Protection must be treated as a package, integrating legal, procedural and psychosocial dimensions.

Culture and training: the invisible infrastructure

No legal framework compensates for toxic organisational culture. Fear, stigma and loyalty-based norms remain major barriers to reporting.

Good practice examples include:

- Mandatory compliance and whistleblowing training;
- Differentiated training for employees, managers, investigators and judges;
- Leadership-level non-retaliation commitments;
- Public campaigns destigmatising whistleblowing;
- Normalisation of whistleblowing in public debate;
- Trauma-informed communication in case handling.

Good practice examples include:

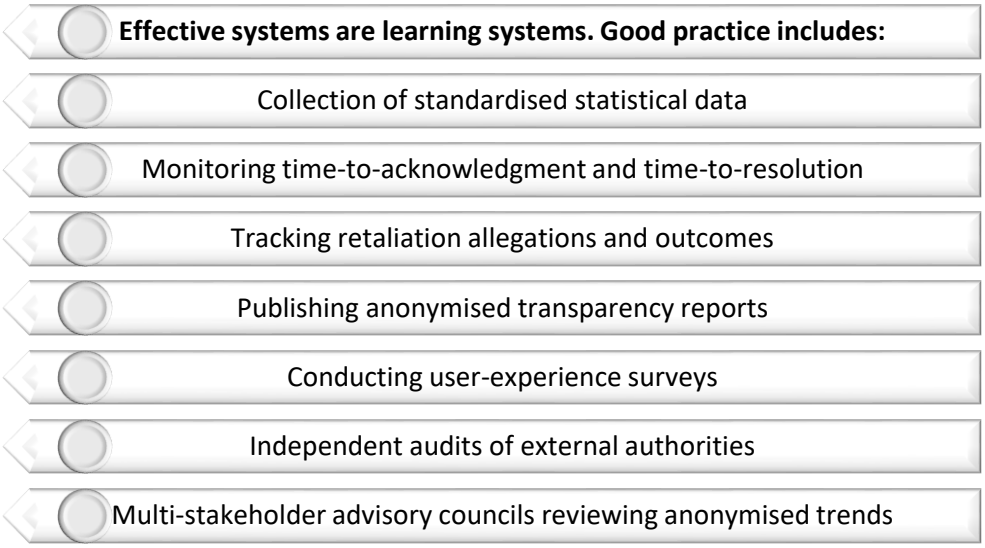
- Mandatory compliance and whistleblowing training
- Differentiated training for employees, managers, investigators and judges
- Leadership-level non-retaliation commitments
- Public campaigns destigmatising whistleblowing
- Normalisation of whistleblowing in public debate
- Trauma-informed communication in case handling

Cultural transformation is gradual but indispensable. Formal channels cannot function effectively in hostile environments.

Monitoring and continuous improvement

Effective systems are learning systems. Good practice includes:

- Collection of standardised statistical data;
- Monitoring time-to-acknowledgment and time-to-resolution;
- Tracking retaliation allegations and outcomes;
- Publishing anonymised transparency reports;
- Conducting user-experience surveys;
- Independent audits of external authorities;
- Multi-stakeholder advisory councils reviewing anonymised trends.



Monitoring transforms compliance into accountability and strengthens institutional credibility.

Strategic conclusions

The central conclusion of the *Good Practice Report* is that effective whistleblower protection is systemic. It cannot rely on isolated legal provisions. It requires coherent interaction between law, institutional design, procedural safeguards, support services, and organisational culture.

Directive (EU) 2019/1937 establishes a floor, not a ceiling. Member States that expanded scope, strengthened institutional independence, and embedded preventive safeguards demonstrate that higher standards are fully compatible with EU harmonisation.

The transformation required is conceptual as well as operational: from reactive compensation to preventive protection; from symbolic compliance to structural credibility; from fragmented remedies to integrated support; from formal channels to trusted systems.

Variation across Member States is analytically valuable. It reveals that failures are not inherent to the Directive but stem from institutional design choices and cultural resistance. Effective protection is achievable.

The *Good Practice Report* therefore provides a practical roadmap for strengthening whistleblower protection across the European Union. Its findings lay the foundation for the forthcoming Policy Recommendations, which will synthesise these insights into concrete reform proposals aimed at closing the persistent gap between formal protection and lived reality

2. Introduction

2.1 Context and Conceptual Framework

From needs analysis to good practice mapping

The VoiceGuard project ("VoiceGuard: Whistleblower Empowerment & Support Initiative") was conceived against a persistent and troubling paradox within the European Union. While the adoption of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (hereinafter "the Directive") marked a historic milestone in harmonising minimum protection standards across Member States, the lived experiences of whistleblowers often remain marked by insecurity, retaliation, and institutional indifference.

The Needs Analysis Report, the first analytical deliverable in the project documented this gap in detail. Drawing on qualitative interviews with whistleblowers and focus groups with professionals across six EU Member States (Czech Republic, Spain, Bulgaria, Romania, Greece, and Luxembourg), the report identified a recurring pattern: formal compliance with the Directive does not automatically translate into effective protection in practice. Reporting channels may exist, but trust is fragile. Legal safeguards may be codified, yet retaliation continues. Remedies may be available, but often only after irreversible personal and professional damage has occurred.

The Good Practice Report builds directly on these findings. If the Needs Analysis identified systemic weaknesses and unmet needs, the present deliverable seeks to answer a complementary question: **What works?** More precisely, which legislative, institutional, procedural, and cultural arrangements demonstrably strengthen whistleblower protection and mitigate the risks identified in the Needs Analysis? And how can these practices be translated into a coherent toolkit to guide Member States, institutions, and organisations toward more effective implementation?

The transition from a needs-based diagnostic to a good practice mapping reflects a deliberate methodological progression within the project. The analytical logic is cumulative:

- Needs Analysis (Deliverable 2.1): Identified gaps between law and practice and mapped the lived experiences of whistleblowers
- Skills Assessment (Deliverable 2.2): Examined capacity constraints among relevant actors.
- Good Practice Report (Deliverable 2.3): Identifies normative and operational models that address the weaknesses previously documented.
- Policy Recommendations (Deliverable 2.4): Will synthesise findings into reform-oriented proposals.

The Good Practice Report therefore does not operate in abstraction. Its conceptual foundation rests on the empirical evidence gathered in the Needs Analysis. It responds directly to identified deficits: procedural hostility, "black hole" reporting channels, retaliation strategies, temporal mismatch between harm and remedy, lack of psychosocial support, and structural conflicts of interest.

The Broader European Context

The Directive established, for the first time, a common European baseline for whistleblower protection. It introduced obligations concerning internal reporting channels, external reporting mechanisms, feedback timelines, confidentiality safeguards, anti-retaliation provisions, and remedies. Importantly, the Directive sets minimum standards, allowing Member States to adopt more favourable provisions.

By the end of 2023, all EU Member States had formally transposed the Directive. However, the pace and depth of transposition varied significantly. Some states adopted minimalist, compliance-oriented frameworks; others used the opportunity to expand material scope, strengthen institutional independence, or introduce stronger enforcement mechanisms.

The Needs Analysis demonstrated that legal transposition alone does not guarantee functional protection. Whistleblowers reported:

- Institutional silence following disclosures
- Hostile organisational cultures
- Discrediting strategies aimed at undermining credibility
- Delayed judicial proceedings
- Financial exhaustion due to litigation
- Psychological trauma resulting from retaliation

At the same time, important geographical contrasts emerged. Luxembourg, for example, was perceived as having a comparatively more functional system, whereas several other Member States exhibited systemic weaknesses. This variation confirms that the Directive's minimum standards are compatible with very different implementation models.

This divergence is analytically valuable. It allows the identification of comparative strengths across jurisdictions. The present report leverages these contrasts to extract replicable elements of effective protection.

The Problem of "Paper Protection"

A central conceptual insight from the Needs Analysis is the distinction between formal protection and effective protection. In many cases, legal safeguards function as what respondents described as a "paper shield." Reporting channels exist, yet whistleblowers distrust them. Anti-retaliation provisions are codified, yet retaliation occurs swiftly and strategically. Courts may ultimately rule in favour of whistleblowers, but only after years of professional exclusion.

This disconnect reveals a structural flaw in systems that rely predominantly on ex post remedies—that is, protection mechanisms activated only after harm has occurred. Such systems presuppose that:

- Whistleblowers can withstand prolonged litigation.
- Retaliatory harm can be reversed through compensation.
- Psychological damage is remediable through legal judgments.

The empirical findings challenge these assumptions. Respondents described retaliation strategies designed not merely to discipline but to destroy professional credibility. The "temporal mismatch" between rapid retaliation and slow legal resolution emerged as a recurrent theme.

Against this background, the Good Practice Report adopts a conceptual shift: **Effective whistleblower protection must move from a predominantly reactive model to a preventive and structural model.**

This does not negate the importance of remedies. Rather, it underscores the need for:

- Early-stage protective measures
- Independent oversight

- Reversal of burden of proof
- Interim relief mechanisms
- Psychosocial support frameworks
- Organisational culture change

The Conceptual Framework presented below is therefore structured around the transformation from formal compliance to substantive protection.

2.2 Conceptual framework

Whistleblowing as a Governance Mechanism

At its core, whistleblowing is not merely an individual act of disclosure. It is a governance mechanism. It operates at the intersection of integrity, accountability, transparency, and institutional trust.

Whistleblowers perform a public function by exposing misconduct that would otherwise remain concealed. In doing so, they serve democratic values, protect public resources, and prevent harm. However, their capacity to fulfil this function depends on institutional conditions.

The Conceptual Framework underpinning this report conceptualises whistleblower protection as resting on five interdependent pillars:

- **Normative Foundations (Legal Scope and Clarity)**
- **Procedural Architecture (Reporting Channels and Case Handling)**
- **Institutional Independence and Capacity**
- **Protection and Support Mechanisms**
- **Organisational Culture and Preventive Environment**

Weakness in any pillar undermines the system as a whole. The Needs Analysis demonstrated that even where normative frameworks are relatively strong, deficiencies in culture, independence, or enforcement can render protection ineffective

Key Definitions and Concepts according to current legal standards

With respect to the ***scope of protection***, as a rule, whistleblower protection covers reports of breaches of law made by persons working in the private or public sector who have acquired information on such breaches in a work-related context.

Several conclusions follow from this definition. First, grievances or complaints that do not refer to breaches of law do not fall within the scope of whistleblower protection. Accordingly, for example, reports expressing dissatisfaction with working conditions, without alleging any breach of law, are not covered by the whistleblowing framework. This distinction is essential in practice, in order to prevent the misuse of whistleblowing channels for matters that should be addressed through ordinary complaint-handling or internal grievance mechanisms.

Second, whistleblower protection applies only to persons who have acquired information on breaches in a work-related context. Therefore, where the reporting person obtained the relevant information outside a professional context, or where the person submitting a complaint acts, for example, as a client of the entity concerned, whistleblower protection legislation does not apply.

A further condition for a reporting person to benefit from the protection afforded by whistleblower protection legislation is that the report was made in ***good faith***. In this regard, the reporting person must have had, at the time of reporting, reasonable grounds to believe that the information reported was true.

This requirement does not imply an obligation for the reporting person to prove the breach, but only to demonstrate a reasonable belief that is based on the information available at the time the report was made. This requirement is not intended to discourage reporting, but rather to ensure that whistleblower protection is not extended to situations in which the reporting person acts in bad faith, for example by deliberately reporting information that they know to be false with the aim of causing harm to another person.

One of the main purposes of the legislation on whistleblower protection is to ensure that the whistleblower is protected from ***retaliation***. As such, it is possible that, as a result of the internal or external reporting or of the public disclosure made by the whistleblower, the entity impacted by such a report or disclosure acts, in a work-related context, in a manner that causes or that may cause an unjustified detriment to the reporting person. Such retaliatory acts must be prevented and it must be ensured that mechanism is put into place so as to remove, to the maximum extent possible, any consequences of such acts.

Retaliation may take various forms, including, for example, suspension, demotion, transfer of duties, change of workplace location, imposition of disciplinary measures, coercion, discrimination, harm to a person's reputation, blacklisting, reduction in wages, negative performance assessment, or failure to renew a fixed-term employment contract. This list is non-exhaustive, as any form of retaliation, including threats of retaliation or attempts thereof, is prohibited.

A breach may be reported through ***internal or external reporting channels*** or by means of ***public disclosure***.

Internal reporting involves the submission of reports through internal channels established by the legal entity. As a general rule, entities in the public sector and entities in the private sector with more than 50 employees are required to establish internal reporting channels. Furthermore, an appropriate procedure must also be put in place in order to ensure that such reporting channels are effective.

As a matter of best practice, reporting through internal channels is generally encouraged as a first recourse, as breaches may be addressed more effectively at organisational level. Such an approach allows organisations to promptly address and remedy breaches while minimising potential harm. However, the use of internal reporting channels is not mandatory, and the reporting person is not required to exhaust internal remedies before making an external report.

External reporting refers to the submission of reports to competent public authorities designated to receive and handle whistleblowing reports. In Romania, such authorities include, depending on the nature of the breach, the authorities legally competent to receive and handle reports in their respective fields, the National Agency of Integrity or other authorities to which the National Agency of Integrity may forward reports for further action.

Whistleblowers may choose to report directly to external authorities, in particular where internal reporting channels are unavailable or where the reporting person reasonably believes that the breach may not be effectively addressed internally or that there is a risk of retaliation.

Public disclosure involves the dissemination of information on breaches of law to the public domain, including through the media or online platforms. Given its potentially significant impact, public disclosure is subject to stricter conditions under whistleblower protection legislation. For instance,

protection may be afforded where the reporting person has previously reported internally and externally or has reported directly externally, and no appropriate action was taken within the applicable timeframe, or where the breach constitutes an imminent danger to the public interest.

The availability of these three reporting avenues reflects a graduated and flexible approach, aimed at ensuring effective reporting while balancing the interests of whistleblowers, organisations and the public.

3. International and European Standards

3.1 The EU Whistleblowing Directive (EU) 2019/1937

With respect to international and European standards, particular importance is attached to the standards established by the EU Whistleblowing Directive (EU) 2019/1937, which ensures a uniform minimum level of protection for whistleblowers across the European Union.

It must be noted from the outset that, as a general rule, the standards laid down by the Directive constitute minimum protection standards. This is expressly stated, inter alia, in the Preamble to the Directive, which provides that:

"*This Directive introduces minimum standards and it should be possible for Member States to introduce or maintain provisions which are more favourable to the reporting person, provided that such provisions do not interfere with the measures for the protection of persons concerned. The transposition of this Directive should, under no circumstances, provide grounds for reducing the level of protection already granted to reporting persons under national law in the areas to which it applies.*"

In the same vein, it is noted in Article 25 of the Directive that:

"*1. Member States may introduce or retain provisions more favourable to the rights of reporting persons than those set out in this Directive, without prejudice to Article 22 and Article 23(2).*

2. The implementation of this Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by this Directive."

With respect to the scope of the Directive, the ***material scope*** is established in Article 2, where it is mentioned that the minimum standards of protection are in place for persons reporting breaches of Union law, breaches that occur in the specific areas mentioned in Article 2[1]. A breach is defined in the Directive as an act or omission that is unlawful and that relates to the Union acts and areas falling within the material scope provided in Article 2 or that defeats the object or the purpose of the rules in the Union acts and areas falling with such a material scope. Further on, it is noted in Article 2(2) of the Directive, that the Member States can extend protection under national law for areas or acts that are not covered in Article 2(1).

[1] "This Directive lays down common minimum standards for the protection of persons reporting the following breaches of Union law:
(a)breaches falling within the scope of the Union acts set out in the Annex that concern the following areas:
(i) public procurement;
(ii) financial services, products and markets, and prevention of money laundering and terrorist financing;
(iii) product safety and compliance;
(iv) transport safety;
(v) protection of the environment;
(vi) radiation protection and nuclear safety;
(vii) food and feed safety, animal health and welfare;
(viii) public health;
(ix) consumer protection;
(x) protection of privacy and personal data, and security of network and information systems;
(b) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures;
(c) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law."

The ***personal scope*** of the Directive is established in Article 4, where it is noted that the Directive shall apply to reporting persons working in the private or in the public sector who obtained the information on breaches in a work-related context[2]. The Directive covers also the scenarios (i) in which the work-based relationship during which the information was obtained has since ended, (ii) in which the work-based relationship is yet to begin and the information has been acquired during the recruitment process or pre-contractual negotiations. Further on, the measures shall also apply for facilitators, third persons who are connected with the reporting persons, such as colleagues or relatives, and who could suffer retaliation in a work-related context and with respect to legal entities that the reporting persons own, work for or are connected with in a work-related context.

The Directive imposes a series of obligations on both private and public sector entities, as well as on competent public authorities, aimed at ensuring effective reporting mechanisms and the protection of whistleblowers.

One of the core obligations introduced by the Directive is the establishment of internal reporting channels and procedures for follow-up. As a general rule, this obligation applies to public sector entities and to private sector entities with 50 or more workers. Internal reporting channels must be designed, established and operated in a secure manner, ensuring the confidentiality of the identity of the reporting person and of any third party mentioned in the report. In addition, an impartial person or department must be designated to receive and follow up on reports, and a reasonable timeframe for providing feedback must be established.

Furthermore, with respect to external reporting, competent authorities are required to establish independent and autonomous external reporting channels to receive and handle reports. Such authorities must diligently follow up on reports and provide feedback to the reporting person within a reasonable timeframe. Where an authority receives a report but lacks competence to address the reported breach, it is required to transmit the report to the competent authority.

Moreover, competent authorities must publish clear and accessible information on their websites regarding, inter alia, the conditions for qualifying for whistleblower protection, the contact details of external reporting channels, the applicable reporting procedures, the confidentiality regime, the nature of the follow-up to be given to reports, and the available remedies and procedures for protection against retaliation.

In addition, authorities must ensure effective protection measures, including the prohibition of retaliation and access to remedies where retaliation occurs.

3.2 Council of Europe Recommendation CM/Rec (2014)7

Another relevant instrument in the field of whistleblower protection is the Recommendation CM/Rec (2014)7 of the Council of Europe. Although non-binding in nature, this instrument has established clear guidelines which have significantly contributed to shaping national legislative frameworks in this area.

[2] „1.This Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following:
(a) persons having the status of worker, within the meaning of Article 45(1) TFEU, including civil servants;
(b) persons having self-employed status, within the meaning of Article 49 TFEU;
(c) shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees;
(d) any persons working under the supervision and direction of contractors, subcontractors and suppliers."

The Recommendation defines a whistleblower as any person who reports or discloses information on a threat or harm to the public interest in the context of a work-related relationship in either the public or the private sector. While the material scope is not exhaustively defined and is left to the discretion of each State, the Recommendation expressly indicates that breaches of law and human rights, as well as risks to public health and safety and to the environment, should be covered by national legislation.

With regard to the personal scope, the Recommendation provides that protection should extend to all individuals working in the public or private sectors. In line with the approach later adopted by the Directive, protection should also apply to individuals whose work-related relationship has ended, as well as to those whose working relationship is yet to begin.

Further on, it is mentioned that the national framework should foster an environment that encourages reporting or disclosure in an open manner. In this respect, it recognizes three main reporting avenues, namely internal reporting, external reporting and public disclosure.

The Recommendation also provides that whistleblowers should be protected against any form of retaliation, including, inter alia, dismissal, suspension, demotion or punitive transfers.

As can be observed, the Recommendation sets out less detailed and less stringent requirements than those established by the Directive. Nevertheless, several of the core principles and safeguards promoted by the Recommendation have subsequently been incorporated into the Directive.

3.3. United Nations Convention against Corruption (UNCAC)

Whistleblower protection is also addressed at the level of the United Nations through the UNCAC.

In this respect, Article 8(4) provides that each State Party shall consider establishing measures and systems to facilitate the reporting by public officials of acts of corruption.

Furthermore, Article 33 expressly provides that each State Party shall consider incorporating into its domestic legal system appropriate measures to protect persons who, in good faith and on reasonable grounds, report to the competent authorities facts concerning offences established in accordance with the Convention, against any unjustified treatment.

As can be observed, unlike the Directive, UNCAC addresses whistleblower protection in more general terms, by encouraging States Parties to consider adopting protective measures, without imposing detailed or binding obligations in this regard.

3.4. OECD best practice

The OECD best practice guide[3] comprise a detailed comparative analysis of whistleblowing frameworks in a number of jurisdictions, while also identifying key elements that constitute effective protection mechanisms.

In this context, the OECD highlights the importance of clearly defining the categories of disclosures that warrant protection, as legal certainty in this regard is essential for both clarity and public confidence in the whistleblowing framework.

[3] OECD (2016), Commiting to Effective Whistleblower Protection, OECD Publishing, Paris

Further on, it is mentioned that the whistleblower should be protected when acting in good faith, but the onus should not be on the whistleblower to prove the intent of their actions. As measures to discourage bad faith reporting, the OECD best practices refer to: removal of protections, such as confidentiality, libel and defamation suits, or fines.

In addition, the OECD stresses that reporting channels should be clearly defined and designed in a manner that facilitates disclosure. A variety of reporting avenues should be available, allowing whistleblowers to choose, on a case-by-case basis, between internal and external reporting channels.

Confidentiality safeguards are also identified as a core element of effective protection, with the OECD noting that such safeguards should extend to all information that could lead to the identification of the whistleblower.

Moreover, whistleblower protection laws should provide comprehensive protection against discriminatory or retaliatory personnel actions, as well as against threats of reprisal. In this respect, the OECD underlines that the mere existence of reporting channels does not, in itself, amount to protection. Effective protection against retaliation requires, inter alia, the reversal of the burden of proof, given the practical difficulties whistleblowers may face in demonstrating a causal link between the disclosure and the retaliatory action.

Considering the lengthy duration of retaliation proceedings, the OECD further highlights the importance of access to interim relief measures for whistleblowers who suffer reprisals as a result of making a protected disclosure. It is also noted that reinstatement as a remedy for reprisal is the norm, whereas remedies could also consist in compensation or punitive damages.

Finally, the OECD notes that the use of clear and effective communication methods to inform employees about whistleblowing mechanisms and the protections available to them can foster trust and encourage individuals to raise concerns when they arise.

As can be observed, several of the measures identified as best practices by the OECD have subsequently been incorporated into the Directive, highlighting the importance of such transnational comparative studies in shaping regional whistleblower protection frameworks.

4. Methodology and Analytical Approach

4.1. Research Design and Data Collection Framework

The research design followed a qualitative, comparative, and practice-oriented approach. The objective was not to conduct a statistically representative survey of all EU Member States, but to identify and systematize transferable good practices in the transposition and implementation of Directive (EU) 2019/1937.

The design is rooted in a two-stage analytical progression:

- Stage 1: Diagnostic Baseline – Findings from the Needs Analysis Report, which documented systemic weaknesses, retaliation patterns, institutional bottlenecks, and support gaps across six Member States (Bulgaria, Czech Republic, Greece, Luxembourg, Romania, and Spain).
- Stage 2: Good Practice Mapping – Identification of normative, institutional, procedural, and cultural solutions that address the weaknesses identified in Stage 1.

This cumulative structure ensured that the Good Practice Report is not abstractly normative, but empirically anchored in documented shortcomings.

The research design was structured around five analytical pillars of effective whistleblower protection:

- Normative Scope and Legal Clarity
- Reporting Channels and Accessibility
- Institutional Design and Independence
- Protection Measures and Support Mechanisms
- Implementation, Culture and Monitoring

These pillars mirror the structural gaps identified in the Needs Analysis and serve as organizing principles for both data collection and analysis.

The research design therefore combines:

- Jurisdictions directly studied in the Needs Analysis;
- Additional Member States contributing through TI expertise;
- Cross-country comparative analysis.

4.2. Data collection

Data collection relied on two complementary sources: (A) structured questionnaire responses, and (B) integration of findings from the Needs Analysis, report that was based on systematic consultation of key stakeholders and whistleblowers.

The questionnaire was distributed to:

- All VoiceGuard project partners;
- Transparency International chapters in EU Member States.

This ensured both depth (through project partner jurisdictions) and breadth (through TI's EU-wide network). The inclusion of TI chapters was methodologically significant because many chapters

have practical litigation, advocacy, and advisory experience in whistleblower protection cases, providing practice-based insights beyond formal legislative review.

The questionnaire included in Annex 2 of the current report was designed to collect structured information on national transposition and implementation practices. It was organized across five thematic sections:

- Scope of national legislation
- Protection measures for whistleblowers
- Reporting procedures and channels
- Cooperation with civil society and social partners
- Culture, awareness, and preventive measures

The second data pillar was the systematic valorisation of the Needs Analysis Report. The Needs Analysis had employed:

- 16 in-depth whistleblower interviews;
- multidisciplinary expert focus groups (32 professionals);
- A structured perception questionnaire.

Rather than duplicating data collection, the Good Practice Report conducted a secondary analytical integration of that dataset. Specifically, the Needs Analysis was reviewed to extract:

- Recurring systemic weaknesses;
- Documented retaliation patterns;
- Identified protection gaps;
- Reported failures of reporting channels;
- Observed geographical contrasts.

This consultation process served two methodological functions:

- Problem Identification: Clarifying which failures require good practice responses.
- Validation Benchmark: Assessing whether identified "good practices" plausibly address empirically documented problems.

This approach ensures that good practices are functionally responsive rather than merely formally compliant.

4.3. Data Analysis Approach

The data analysis combined comparative legal analysis, thematic qualitative synthesis, and problem-solution mapping. Each responding Member State's framework was analysed against:

- Minimum requirements of Directive (EU) 2019/1937;
- OECD best practice standards;
- Council of Europe Recommendation CM/Rec(2014)7.

Questionnaire responses were organized in structured analytical tables corresponding to the five pillars of effective protection and the mapping elements identified:

- Minimum-compliance approaches;

- Expanded-scope approaches;
- Innovative institutional arrangements;
- Gaps or inconsistencies.

A distinctive feature of this methodology is the direct linkage between the empirically identified failures (as described in the Needs Analysis) and the documented effective practice resulting from the collected data.

4.4. Data Quality and Limitations

The methodology adopted for the Good Practice Report combines structured comparative inquiry with empirical grounding in whistleblower experiences. By integrating questionnaire-based cross-country mapping with consultation of the Needs Analysis, the research design ensures that identified good practices are:

- Normatively sound;
- Institutionally feasible;
- Empirically responsive;
- Transferable across EU Member States, subject to contextual adaptation.

The resulting analysis moves beyond formal compliance assessment toward identifying operational models capable of transforming "paper protection" into substantive, preventive, and enforceable whistleblower safeguards.

Several methodological limitations must be acknowledged:

- **Non-representative sample.** The questionnaire relied on project partners and TI chapters, and a limited number of answers was received, rather than a statistically representative sample of all competent authorities. Findings therefore reflect informed expert perspectives rather than full institutional surveys.
- **Variability in detail.** Responses varied in depth and specificity. Some jurisdictions provided extensive legislative and operational detail; others offered more general assessments.
- **Difference between the implementation and the formal legal provisions.** As highlighted in the Needs Analysis, a central challenge is the gap between law-on-the-paper and law-in-practice. Questionnaire responses may sometimes reflect formal compliance rather than everyday operational reality.
- Evolving institutional frameworks. In several Member States, competent authorities (e.g., newly established whistleblowing offices) are still operationalizing their mandates. Some practices are therefore evolving and not yet fully tested.
- **Contextual dependency.** Certain practices (e.g., centralized oversight models) may depend on administrative traditions, legal culture, or institutional capacity specific to a jurisdiction. Replicability must therefore consider contextual adaptation.

5. Core Pillars of Effective Whistleblowing Protection

5.1. Normative Foundations

Wide material and personal scope of the law

A core element of effective protection is a broad and clear material and personal scope. Restrictive definitions create uncertainty and discourage reporting.

Good practice examples identified across Member States include:

- **Extension of material scope beyond EU law to encompass national law violations.**
- **Inclusion of labour law breaches, serious misdemeanours, and public interest wrongdoing.**
- **Broad personal scope covering employees, former employees, contractors, trainees, volunteers, and facilitators.**

A consistent good practice is to define the material scope broadly (covering breaches of both EU and national law, as well as wider "public interest" wrongdoing), beyond the minimum required by Directive (EU) 2019/1937.

A narrow scope produces fragmentation and artificial distinctions between "protected" and "non-protected" wrongdoing. This weakens legitimacy and creates legal ambiguity.

The Directive permits broader national provisions. Good practice jurisdictions use this flexibility strategically.

Bulgaria broadened the scope to include breaches of Bulgarian legislation, criminal offences of a general nature, and labour law violations.

The Czech Republic's legislation also exceeds the Directive's minimum by covering misdemeanours with fines above a defined threshold, effectively bringing most serious labour-related violations within the protection regime. This extended scope enhances accessibility and avoids artificial distinctions between "protected" and "non-protected" wrongdoing, strengthening the system's credibility.

Luxembourg's transposing law (16 May 2023) is described as intentionally broad and adaptable, and Sweden's approach is a good practice for covering disclosures that are of "public interest" rather than restricting protection to narrow categories and law infringements. This mirrors European good practice under the EU Whistleblowing Directive, which requires protection for a wide range of "reporting persons" connected to a work context, and encourages Member States to avoid overly restrictive definitions that deter reporting.

In France, the legal framework is designed to ensure a general, cross-sectoral regime rather than a narrow, sector-by-sector patchwork. The law transposing the European Directive 2019/1937 adopts a horizontal approach (i.e., not limited to specific domains).

On the other hand, the definition of a broad personal scope, as intended by the Directive, is important, covering not only employees, but also former employees, applicants, contractors, suppliers, volunteers, trainees, shareholders, and other work-related actors.

That French law protects not only whistleblowers but also facilitators, connected persons (e.g., colleagues/relatives), and legal entities linked to the whistleblower, and it treats civil society

organisations providing advice as covered through the "facilitator" concept. This is a strong design choice: retaliation often targets the whistleblower's network, not only the individual.

Following the Directive, the laws in EU countries cover both public and private sectors. This is a major good practice because it avoids gaps where certain types of wrongdoing or certain categories of organisations fall outside protection.

Reasonable belief standard

The protection of individuals who report based on "reasonable grounds to believe" that information is true is a cornerstone of effective frameworks.

In most of the EU countries the legal texts or practices point to the importance of protecting people who report *in good faith based on what they could reasonably believe at the time*, rather than requiring them to "prove" the breach. A good practice formulation is to protect disclosures where the reporting person had reasonable grounds to believe the information was true and within scope, even if an investigation later finds no breach. Transparency International's guidance frames "reasonable belief" as a core safeguard because it encourages early reporting and reduces chilling effects created by fear of liability.

In this framework of good practices**, protection must not depend on the ultimate confirmation of wrongdoing. Otherwise, individuals are deterred from reporting early-stage concerns.**

Good practice approaches operationalise this standard through:

- **Interpretative guidance favouring protection in doubtful cases (*in dubio pro* whistleblower).**
- **Clear differentiation between mistaken reporting and malicious false reporting.**
- **Proportionate sanctions for demonstrably bad-faith disclosures, without chilling legitimate reports.**

The Czech Ministry of Justice's recommendation of an in *dubio pro whistleblower* approach reflects an important good practice. This principle advises competent persons to treat uncertain cases as protected disclosures where reasonable doubt exists. Such interpretative guidance operationalizes the reasonable belief standard and prevents overly restrictive readings of the law.

The French approach also anchors protection in the whistleblower having reasonable grounds to believe the information was true at the time of reporting—meaning protection should not depend on whether wrongdoing is ultimately proven. Case-law from France shows that a judgement of bad faith requires proof of knowledge of falsity, not merely that allegations are not established.

Clear anti-retaliation provisions

The prohibition of retaliation must be more than declaratory. Effective systems integrate:

- **Detailed non-exhaustive lists of prohibited retaliatory acts.**
- **Coverage of attempted retaliation and threats.**
- **Protection of facilitators and related persons.**
- **Reversal of burden of proof in retaliation disputes.**

Strong practice is to prohibit retaliation in a detailed, operational way, listing common retaliatory acts (dismissal, demotion, negative evaluations, blacklisting, harassment, threats, litigation intimidation), explicitly covering attempted retaliation, and extending protection to facilitators and related persons.

Luxembourg is providing robust protection beyond the reporter alone (including colleagues/relatives and those facilitating reporting), which reflects the Directive's approach to protecting both the reporting person and connected persons who may be targeted.

Spain codified and expanded an existing judicial doctrine of indemnity that had previously been limited mainly to labour contexts.

On the other hand, in Greece, professional stakeholders emphasized the need for clearly defined statutory clauses guaranteeing protection for a defined period following a report (a form of "lock-out" period). The clarity and predictability of protection measures are central to building trust.

Burden of proof reversal

One of the clearest "high-value" legal design features is the *reversal (or shifting) of the burden of proof* in retaliation disputes. This reversal of burden of proof is particularly significant. Without it, whistleblowers face evidentiary barriers in proving causation between disclosure and adverse action.

Luxembourg provides a model example through the presumption of retaliation, shifting the burden of proof to the employer if detrimental measures follow a report. This significantly lowers evidentiary barriers for whistleblowers and acts as a strong deterrent against reprisals. Such reversal transforms protection from a declarative principle into an enforceable safeguard. This aligns closely with OECD good practice, which stresses that shifting the burden is necessary because whistleblowers often cannot access evidence needed to prove causation.

5.2. Reporting Channels and Accessibility

Internal reporting channels established based on consultations and capacity

Best practice requires that these channels function as protective mechanisms rather than merely compliance tools. According to the Directive, multi-channel reporting model with defined timelines provides clarity and predictability.

The strongest internal-channel practices combine clear legal duties with practical implementation supports. However, internal arrangements introduced without meaningful worker consultation or trust-building can undermine credibility. **A good practice, therefore, is to involve worker representatives early** (where relevant), publish clear explanations of how confidentiality is protected, and demonstrate that reports lead to action. This is a good practice that was flagged in Romania in some institutions.

Moreover, in Romania, Municipalities under thresholds (fewer than 10,000 inhabitants or fewer than 50 workers) may group together and share resources for receiving reports and follow-up. This is a good practice because it recognises capacity constraints and enables functional compliance.

External reporting accessibility

A core good practice present in Romania and France, among others, is the fact that whistleblowers can chose to report directly externally without imposing extra conditions, or with conditions that are only dependent on the whistleblowers' assessment of their situation. This ensures a higher level of trust for the whistleblowers, that often mistrust the confidentiality and independence of internal channels, especially if the leadership of their institution or firm is perpetrating wrongdoings that are the object of the report.

Greece designated the National Transparency Authority as an external channel, offering an alternative when trust in internal systems is low. In Bulgaria, the Personal Data Protection Commission functions as the central external channel, with oversight from the Ombudsman. In Romania, the National Integrity Agency functions as the main external channel, with additional sectoral institutions already specialized in dealing with citizens' complaints or reports also acting as external channels for their specific domains.

Luxembourg's designation of 22 competent authorities generate some confusion among whistleblowers and may act as a deterrent However, the existence of the Office for Whistleblowers, accessible via Guichet.lu, reduces uncertainty and signals institutional ownership.

Spain's legal structure permits reporting to national or regional authorities, demonstrating decentralised access.

Conditions for public disclosure

Public disclosure (e.g., to media or the public) appears as a sensitive point where overly restrictive rules can weaken protection in exactly the circumstances when trust in internal/external channels is low. The EU Directive protects public disclosure under defined conditions (for example, where internal/external reporting did not lead to appropriate action within timelines, or where there is imminent danger to the public interest), aiming to balance accountability and fair process. However, in practice, this may discourage whistleblowers. A good practice is to make these conditions clear, realistic, and communicable, so whistleblowers are not forced into legal uncertainty when deciding whether escalation is necessary.

Anonymous and confidential reporting

A distinction should be made between confidentiality (protecting identity) and anonymity (not collecting identity). Several countries allow for anonymous reporting, as long as the reports are detailed enough to allow authorities to start an investigation.

The creation of secure digital platforms enabling anonymous two-way communication is identified as a strong good practice, particularly in Greece and large private-sector organizations.

On the other hand, a good practice is to ensure it is "real" anonymity (no metadata leakage, secure vendor arrangements, and controlled access). ISO 37002–aligned approaches emphasize trust and protection as foundational principles, which in practice means designing reporting tools and workflows that minimise identity exposure and restrict access to those with a need to know.

Accessibility (language, disability, digital access)

Variability (depending on internal procedures of institutions and companies) usually defines the accessibility of reporting channels. Good systems are those perceived as user-friendly in practice. A strong accessibility approach is to provide multiple channels (digital, phone, in-person), plain-language guidance, options in relevant languages, and accommodations for disability (including accessible web design and alternative formats).

Bulgaria's example of a multi-channel corporate system (phone/online/in-person) illustrates a practical direction: accessibility improves when the reporting experience is simple, predictable, and safe, not merely legally available.

Good practices include also digital platforms with structured forms (for example in Greece and Romania), standardized reporting templates (provide by external authorities in all countries studied), and accessible public guidance (Luxembourg's Guichet.lu service pathway).

Case Handling, Investigation and Due Process

Strong legal rules must be converted into reliable operational practice. ISO 37002 usefully frames whistleblowing management as a lifecycle—receiving, assessing, addressing, and concluding cases—anchored in trust, impartiality, and protection.

Good practices in case handling therefore include:

- **structured intake and triage (including eligibility checks and urgency screening),**
- **early risk assessment (retaliation, safety, evidence preservation),**
- **clear investigation standards (proportionality, confidentiality, competent investigators, and documented reasoning),**
- **procedural fairness for all parties (including the subject of the report).**

Systems are also stronger when documentation is traceable (audit trails for access and decisions) and when timelines and feedback are predictable—both to build trust and to reduce the temptation toward premature public disclosure.

Czech methodological guidance for "Relevant Persons" provides structured case management tools and interpretative materials.

Moreover, the Czech Republic's growing body of case law, including Supreme Administrative Court decisions scrutinizing potential retaliatory measures, reflects an effective judicial oversight function. Also, timely judicial handling in Czech cases (e.g., Kodym) demonstrates responsiveness.

A good practice emerging from case law in Romania is recognition that requests under the whistleblower law should be handled via the special procedure referenced by Law 361/2022 (interim injunction / ordonanță prezidențială), not diverted into slower frameworks. The Constanța Court of Appeal decision highlighted in the report held that the whistleblower is not required to provide a perfect legal classification or exhaustive framing; authorities carry responsibility for legal qualification and substantive assessment. This is an additional good practice because overly technical expectations deter reporting and favour insiders with legal support.

5.3. Institutional Design and Independence

Reporting systems fail where conflicts of interest undermine trust. Good practice features include:

- **Independent external authorities with investigative powers.**
- **Clear mandates and public guidance.**
- **Budgetary and functional autonomy.**
- **Transparent appointment procedures.**
- **Specialised case handlers trained in confidentiality and trauma sensitivity.**

External reporting to competent authorities

Good practice is to designate competent authorities with a clear mandate covering intake, triage, confidentiality, feedback, and referral/investigation powers, and to publish a simple "map" of which authority handles what. Where multiple authorities exist, clarity prevents misdirected reports and lost time—an issue that can become acute in urgent cases.

Institutional credibility is not symbolic—it directly shapes reporting behaviour.

Italy's anti-corruption authority model, and Spain's independent anti-fraud body (Valencian AVAF) with investigative capacity are good practice in choosing the institution responsible for the external reporting channel. Good practice here is not just naming an authority, but ensuring it has budget, trained case handlers, secure intake tools, and legal powers to obtain information and protect reporters.

Independence and safeguards against conflicts of interest

Good practice safeguards for the independence and against conflicts of interest to ensure effective protection of whistleblowers include fixed-term leadership with protected tenure, budgetary autonomy, transparent appointment rules, and strong conflict-of-interest rules for case handlers. Council of Europe principles also stress that reporting frameworks should be sensible, practical, and protective: independence is central to credibility. Luxembourg's independent authority with sanctioning powers represents a strong model among the studied cases.

Handling reports involving senior leadership

Even where internal channels exist, systems need a credible path for allegations implicating top management. A good practice is to predefine escalation routes (e.g., direct to an independent external authority, ombudsperson, or external investigator), so reporters are not required to report "up the chain" to the very people implicated. This is one area where ISO-style system design (clear receiving/assessing/addressing steps, impartiality, protection) can be translated into concrete protocols and delegated authorities.

Role of ombudspersons, integrity officers, ethics committees

Where ombudspersons, integrity officers or ethics committees exist, they work best when they are not merely symbolic: they need defined powers, confidentiality duties, and the ability to trigger protective measures and investigations. Integrity officers and ethics structures are most effective when integrated with structured procedures, reporting channels, HR safeguards, and follow-up accountability, all creating an integrity culture.

In Bulgaria, the Ombudsman audits the central external channel, creating an additional accountability layer.

In Romania, the National Integrity Agency (ANI), established as an autonomous administrative authority by Law no. 144/2007, operates independently in investigating unjustified wealth, conflicts of interest, and incompatibilities concerning public officials. Its President and Vice-President are appointed by the Senate following a competitive procedure organised by the National Integrity Council. ANI also functions as the main external reporting channel for whistleblowers. The National Integrity Council, a representative body appointed by Parliament for a four-year term, exercises general oversight over ANI. Under Law no. 144/2007, it organises and validates competitions for ANI's leadership positions, approves the relevant procedures, and reviews managerial and external audit reports. This structure balances ANI's operational independence with institutional accountability and strengthens public trust in the integrity framework. While whistleblowers may normally submit reports to ANI when they do not trust internal channels within their own institutions, Law no. 361/2022 provides a specific safeguard for cases concerning ANI's own management: in such situations, the National Integrity Council must apply a dedicated procedure for handling reports related to ANI's leadership, ensuring effective protection for employees and other persons in a professional relationship with the Agency and preventing conflicts of interest.

Use of external investigators

A good practice (especially relevant to sensitive cases) is to allow independent investigators, either as a standing option or when conflicts arise. This is particularly important for allegations involving senior leadership, high reputational risk, or complex evidence, where internal impartiality is hard to guarantee.

5.4. Protection Measures and Support Mechanisms

Protection Measures and Support Mechanisms

A good practice model is a package of protections rather than a single remedy:

- **Interim protective measures (rapid steps to prevent dismissal or harassment),**
- **Early access to legal aid**
- **Workplace adjustments (temporary reassignment at the whistleblower's request, remote work options, changes to reporting lines),**
- **Access to psychological support,**
- **Accredited support networks,**
- **Clear long-term remedies (regulated nullity of all retaliation acts and compensations guaranteed.**

Luxembourg's whistleblowers protection system explicitly links legal and psychological assistance to this framework, illustrating how support services can be treated as part of protection rather than an afterthought.

But, although protection measures and support mechanisms are key for the effectiveness of whistleblowers protection, some jurisdictions rely on NGOs/unions for advice, while formal legal aid may be absent or limited.

The whistleblowers protection framework in France is strong in prohibiting retaliation, using a broad formulation (capturing "any prejudice" or unfair/disadvantageous treatment), covering direct and indirect retaliation, threats/attempts, and retaliation outside a strict work-context—plus retaliation by actors other than the employer. This breadth is a key good practice: retaliation is adaptive and often subtle; narrow lists miss real harms. An important good practice in France is the presumption of retaliation once the whistleblower establishes reporting and detriment, with the burden shifting to the employer/actor to justify the measure on duly justified grounds.

Still in France competent authorities may provide (sometimes jointly) psychological support and temporary financial assistance when the whistleblower's situation has seriously deteriorated due to reporting; it also notes judicial possibilities for provisional allocations in proceedings. While this support may be still insufficient (needing additional arrangements, such as a single access point, systematic legal aid), the existence of these support hooks is still a good practice foundation.

In Romania, the support mechanism includes, according to the law:

- Counselling/information and assistance before authorities from the National Integrity Agency;
- Legal assistance for whistleblowers in disciplinary proceedings and when challenging retaliation, following the procedures for court-appointed lawyer (public defenders) in all legal proceedings before the courts.
- The possibility of conducting an open disciplinary procedure when a whistleblower is accused of disciplinary misconduct. This includes allowing the whistleblower to invite a trade union representative, journalists, and/or NGO representatives to attend the proceedings. Such transparency helps reduce the risk of abuse and strengthens procedural safeguard.

Protection of third parties

Another strong practice is protecting related persons and facilitators (colleagues, relatives, union representatives, and those receiving/handling reports) because retaliation often targets a wider circle. This also aligns with the Directive's recognition that protection should extend beyond the primary reporter.

Timely and effective remedies

Finally, remedies must be realistically obtainable: reinstatement, compensation, and penalties for retaliators become meaningful when procedures are simple, burdens of proof are workable, and decision-makers have authority to grant timely relief—an approach also emphasised in OECD best-practice guidance on anti-retaliation systems.

Luxembourg's framework allows retaliatory measures to be declared null and void and provides for compensation. This reinforces practical protection.

Bulgaria and Romania introduced administrative fines for natural and legal persons violating whistleblower protections.

A notable judicial good practice from the Czech Republic demonstrates timely court decisions in whistleblower cases, reinforcing the effectiveness of remedies in practice.

6. Implementation, Culture and Effectiveness

6.1. Training, Awareness and Organizational Culture

Training and awareness building

Training is essential both for fostering an organizational culture that encourages the reporting of wrongdoing and protects whistleblowers, and for strengthening the capacity of responsible staff to handle reports properly, ensure confidentiality, and provide effective protection.

In France there is a mandatory corporate compliance expectation under Sapin II concerning the training on Whistleblowers protection. Established training programmes for key roles also exist in Luxembourg. The Czech Ministry of Justice trained over 560 professionals and issued detailed methodological guidance, representing a strong implementation practice.

The common good-practice thread in countries where training and awareness building are systematic is to train different groups differently:

- **broad staff awareness (how to report, what happens next, what protection means),**
- **manager training (how to respond, prevent retaliation, and avoid "informal reprisals"),**
- **specialised training for case handlers/investigators/judges (confidentiality, trauma-informed communication, evidence handling, and reasoned decision-making).**

Building the protective organisational culture

Culture-focused measures matter because fear and stigma are repeatedly implied by stakeholders interviewed for the needs assessment. Formal mechanisms cannot compensate for toxic cultures. A system perceived as hostile will be bypassed. Cultural transformation is slow, but it is indispensable. The absence of a speak-up culture emerged as a critical barrier in multiple Member States.

Good practice in integrity culture is practical and visible: leadership "tone from the top," non-retaliation commitments backed by consequences, and credible examples showing that reports lead to corrective action. Among the studied countries, Spain reports normalization of whistleblowing in public debate, indicating cultural shift. ISO 37002–type approaches explicitly treat trust and protection as system principles, which can be operationalised through leadership messaging combined with measurable internal accountability.

6.2. Monitoring, Evaluation and Continuous Improvement

A good practice response is to build a learning system:

- **collect standardised data (volumes, channel usage, time-to-acknowledge, time-to-close, substantiation rates, retaliation allegations, outcomes);**
- **measure trust and user experience (surveys, exit interviews, focus groups);**
- **publish transparency reports that protect confidentiality while demonstrating system effectiveness.**

Independent audits or reviews—especially of external authorities' capacity and independence—help prevent "paper compliance."

Council of Europe work on whistleblower protection underscores that frameworks should be practically usable by governments and stakeholders, which is best achieved when monitoring results are used to continuously adjust procedures, resources, and public communication.

Multi-stakeholder councils exist in several countries (e.g., Spain and Luxembourg), the good practice is to use these bodies as genuine "learning loops":

- reviewing anonymised case trends;
- recommending legislative/procedural changes;
- coordinating awareness work with civil society and professional associations.

7. Conclusions

From Formal Transposition to Substantive Protection

The adoption of Directive (EU) 2019/1937 marked a historic milestone in European whistleblower protection. For the first time, a harmonised baseline of safeguards was established across the European Union, covering reporting channels, confidentiality, anti-retaliation measures, and access to remedies. As documented throughout this Good Practice Report, all Member States have formally transposed the Directive. However, the core question underpinning this deliverable was never whether transposition occurred—but whether protection works in practice.

The analysis conducted within the Needs Analysis report demonstrates that the quality of implementation varies significantly across jurisdictions, but it is generally no generating the expected results. Formal compliance does not automatically translate into effective protection. Legal frameworks may exist on paper, but their operationalisation depends on institutional design, procedural safeguards, cultural context, and political will.

This report therefore moved beyond formal legal mapping toward identifying concrete, operational good practices capable of transforming minimum standards into functional systems. The conclusions drawn here synthesise those findings and articulate a strategic direction for strengthening whistleblower protection across the EU.

The central conclusion is clear: effective whistleblower protection is not achieved through isolated legal provisions, but through coherent, interdependent systems built on five mutually reinforcing pillars:

- **normative clarity,**
- **accessible reporting architecture,**
- **institutional independence,**
- **comprehensive protection measures,**
- **a culture of integrity.**

Weakness in any one of these pillars undermines the entire framework.

Variation across Member States is not merely a problem—it is a resource. Divergence reveals which practices strengthen systems and which leave them vulnerable. The contrast between more functional systems and those struggling with implementation confirms that effective protection is achievable within the Directive's framework. Failures are not inherent to EU law; they are products of institutional design choices and cultural resistance.

The Directive establishes, therefore, a floor, not a ceiling. Member States that strategically expanded scope, strengthened institutional independence, and embedded preventive safeguards demonstrate that higher standards are compatible with EU harmonisation.

From Reactive to Preventive Systems

A recurring theme across jurisdictions is the predominance of reactive protection models. In many Member States, remedies are primarily activated after retaliation occurs—through litigation,

compensation claims, or administrative review. While such remedies are essential, they are insufficient.

The empirical evidence underlying this report demonstrates that retaliation often unfolds rapidly and strategically. By contrast, judicial proceedings and administrative investigations move slowly. This temporal mismatch produces a structural imbalance. Whistleblowers may ultimately obtain favourable decisions, but only after years of professional marginalisation, financial strain, and psychological harm.

The strongest good practices identified in this report share a common feature: they shift the focus from ex post compensation to ex ante protection.

Examples include:

- Reversal of the burden of proof in retaliation disputes;
- Interim relief mechanisms preventing dismissal or disciplinary action;
- Early risk assessment during case intake;
- Presumptions of retaliation when detriment follows reporting;
- Explicit nullity of retaliatory acts.

These mechanisms alter incentives. They signal that retaliation carries immediate consequences. They reduce evidentiary barriers faced by whistleblowers. They rebalance procedural asymmetry between individuals and institutions.

The transformation from reactive to preventive protection is not merely a legal refinement—it is a structural reorientation of the whistleblower protection paradigm.

Normative Foundations: Breadth, Clarity and Legal Certainty

The first pillar of effective protection lies in normative design. Narrow material or personal scope creates fragmentation, artificial distinctions, and legal uncertainty. Broad, cross-sectoral frameworks enhance legitimacy and accessibility. The comparative analysis highlights several good practices in this domain:

- Extension of protection beyond EU-law breaches to encompass violations of national law;
- Inclusion of labour law infringements and public-interest wrongdoing;
- Protection of facilitators, related persons, and legal entities connected to the whistleblower;
- Cross-sectoral, horizontal legislative approaches.

A broad personal scope is particularly important. Retaliation frequently targets not only the reporting individual, but colleagues, relatives, or support actors. Legal frameworks that recognise this dynamic—by protecting facilitators and connected persons—demonstrate greater realism and systemic coherence.

Equally critical is the reasonable belief standard. Good practice ensures that protection does not depend on the ultimate confirmation of wrongdoing. Otherwise, individuals are deterred from reporting early-stage concerns. Interpretative principles such as *in dubio pro whistleblower* strengthen legal certainty and encourage responsible disclosure.

Reporting Channels: Accessibility, Trust and Functional Design

Normative breadth, however, must be accompanied by clarity. Legal definitions, public guidance, and procedural explanations must be accessible and comprehensible. Ambiguity deters reporting. Complexity privileges insiders with legal expertise. Simplicity enhances trust.

The existence of reporting channels is not sufficient. Their credibility determines their use. This report identified strong good practices in jurisdictions where reporting architecture reflects the following characteristics:

- Multi-channel access (digital, telephone, in-person);
- Secure digital platforms enabling anonymous two-way communication;
- Clear timelines for acknowledgment and feedback;
- Structured intake procedures;
- Transparent escalation pathways for cases implicating senior leadership;
- Plain-language public guidance;
- Accessibility accommodations for disability and linguistic diversity.

A particularly important conclusion concerns anonymity and confidentiality. These concepts are distinct but complementary. Confidentiality protects identity; anonymity avoids collecting it. Systems that offer secure anonymous reporting mechanisms increase perceived safety, especially in environments characterised by low trust. However, anonymity must be technically credible. Secure vendors, metadata protection, restricted access, and audit trails are not luxuries—they are prerequisites for trust.

External reporting channels play an equally important role. In contexts where internal channels are perceived as compromised or aligned with management, external authorities must provide a credible alternative. Good practice includes:

- Clear designation of competent authorities;
- Published guidance mapping which authority handles which type of report;
- Sufficient investigative powers;
- Budgetary autonomy;
- Trained case handlers;
- Confidential intake procedures.

Confusion regarding competent authorities undermines reporting. Simplicity strengthens accessibility.

Public disclosure remains a sensitive escalation mechanism. Rules must strike a balance between accountability and procedural fairness. Overly restrictive conditions discourage whistleblowers in precisely those circumstances where internal and external channels fail. Clear, communicable standards are essential.

Protection Measures: From Fragmented Remedies to Integrated Support

Protection must be understood as a package—not a single remedy. Effective systems combine:

- Interim protective measures;
- Reversal of burden of proof;

- Nullity of retaliatory acts;
- Access to legal aid;
- Transparent disciplinary procedures;
- Psychological support;
- Temporary financial assistance where necessary;
- Protection of third parties and facilitators;
- Administrative sanctions for retaliators.

The integration of legal and psychosocial support is particularly significant. Retaliation frequently produces psychological harm. Protection frameworks that recognise this dimension demonstrate greater systemic maturity.

Transparency within disciplinary proceedings—such as allowing union or NGO observers—reduces abuse and reinforces fairness.

Administrative fines and sanctioning powers create deterrent effects, reinforcing that retaliation is not cost-free.

Institutional Design: Independence as a Precondition for Credibility

Institutional credibility directly shapes reporting behaviour. Whistleblowers assess not only legal rules, but institutional integrity. Independent anti-corruption authorities, whistleblowing offices, and integrity agencies provide stronger external reporting environments than diffuse or politically controlled structures. Independence must not be symbolic. It should be operational.

Good practices in institutional design include:

- Fixed-term leadership with protected tenure;
- Transparent appointment procedures;
- Budgetary autonomy;
- Clear investigative mandates;
- Conflict-of-interest safeguards;
- Oversight mechanisms balancing independence with accountability.

Handling allegations against senior leadership requires particular attention. Good practice predefines escalation routes to independent bodies, preventing situations where whistleblowers must report "up the chain" to those implicated.

The role of ombudspersons, ethics committees, and integrity officers is effective only when these actors possess defined powers and procedural authority, not merely advisory status.

Culture: The Invisible Infrastructure of Protection

No legal framework can compensate for toxic organisational culture. Formal systems fail where reporting is stigmatised as betrayal rather than recognised as civic responsibility. Good practices in cultural transformation include:

- Leadership "tone from the top";
- Explicit non-retaliation pledges backed by consequences;

- Public examples demonstrating corrective action;
- Normalisation of whistleblowing in public discourse;
- Mandatory training programmes;
- Differentiated training for staff, managers, and investigators;
- Trauma-informed communication practices.

Training must be systematic and role-specific. Broad awareness for employees must be complemented by specialised training for case handlers, investigators, judges, and HR professionals.

Monitoring and Continuous Improvement

Cultural change is gradual. However, jurisdictions where awareness campaigns, professional training, and political leadership support converge demonstrate stronger reporting environments. Effective protection systems are learning systems. Good practice includes:

- Collection of standardised statistical data;
- Monitoring time-to-acknowledgment and time-to-resolution;
- Tracking retaliation allegations;
- Publishing anonymised transparency reports;
- Conducting user-experience surveys;
- Independent audits;
- Multi-stakeholder advisory councils reviewing anonymised case trends.

Monitoring transforms compliance into accountability. Transparency builds trust. Data-driven adjustments improve resilience.

Systems must evolve in response to evidence. Static frameworks stagnate.

The Strategic Path Forward

The cumulative findings of this report point toward a strategic direction for strengthening whistleblower protection across the European Union:

i. **Embed preventive safeguards** (burden shifting, interim relief, early risk assessment).
ii. **Strengthen institutional independence and capacity**.
iii. **Ensure broad, clear legal scope**.
iv. **Design accessible, secure reporting architecture**.
v. **Integrate psychosocial support** into protection frameworks.
vi. **Invest in cultural transformation** through training and awareness.
vii. **Build monitoring and learning mechanisms**.

8. Annexes

8.1. Annex 1. Toolkit for Whistleblower Protection

EU Legislation and resources

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law

Report on the transposition of the Whistleblower Protection Directive (Directive 2019/1937 (EU)) on the protection of persons who report breaches of Union law

Guidelines

Assessing whistleblowing legislation: methodology and guidelines for assessment against the EU Directive and best practice

Published on: 23 September 2020

By: Transparency International

Blueprint principles for whistleblower protection

Published in: 2021

By: Blueprint for Free Speech

Monitoring internal whistleblowing systems

Published on: 10 June 2025

By: Transparency International Ireland

Publicising an alert: media coverage for journalists and whistleblowers

Published on: 22 April 2025

By: La Maison des Lanceurs d'Alerte

Guide to EU Directive on Whistleblower Protection Key Elements relevant to Public Procurement

Published in: 2019

By: Access-Info Europe

Reports

Internal whistleblowing systems: Self-assessment framework for public and private organisations

Published on: 31 October 2024

By: Transparency International

Internal Whistleblowing Systems: Best practice principles for public and private organisations

Published on: 02 November 2022

By: Transparency International

How well do EU countries protect whistleblowers? Assessing the transposition of the EU Whistleblower Protection Directive

Published on: 07 November 2023

By: Transparency International

Are whistleblowing laws working? A global study of whistleblower protection litigation

Published on: 2 March 2021

By: Government Accountability Project & International Bar Association

Speak Up Report 2025

Published on: 3 November 2025

By: Transparency International Ireland

Following-up on whistleblowing reports: a comparative analysis of models adopted by selected european countries

Published in: February 2025

By: NEIWA & Slovakian Whistleblower Protection Office

Stakeholder Mapping and Civil Society initiatives focusing on gender and whistleblowing

Published on: 29 August 2024

By: University of Galway

Finding a voice, seeking justice: The barriers women face to reporting corruption in the European Union

Published on: 18 October 2021

By: Transparency International

Tools

Assessing Whistleblowing Legislation: Methodology and Guidelines for Assessment Against the EU Directive and Best Practice

Published on: 23 September 2020

By: Transparency International

Practical toolkit for developing whistle-blower protection frameworks

Published in: 2025

By: UNODC, Government Accountability Project, European Commission

Whistleblowing toolkit

Published on: 03 December 2020

By: Eurocadres

Resources for business sector

Whistleblowing Guidelines

Published on: 26 September 2024

By: AmCham Romania

Whistleblowing in European companies - Industrial relations for successful implementation of reporting channels

Published in: October 2021

By: EUROCADRES

8.2. Annex 2. Questionnaire on good practices in the transposition and implementation of the EU Directive 2019/1937 on the protection of persons who report breaches of Union law ("the Whistleblowing Directive")

- *If the question to an answer is „YES", please provide more information or links to useful documents*
- *If the question to an answer is „NO", no additional information is needed*

i. **Scope of National Legislation**

- **Broad Material Scope**: Is the national legislation covering a broad material scope?
- **Forward-looking Provisions**: Is the national legislation forward-looking?

ii. **Protection Measures for Whistleblowers**

- **Remedies and Redress**: Are remedies and redress measures well adapted to the needs of whistleblowers?
- **Confidentiality Guarantees:** Are the rules on confidentiality strict and broad enough to offer effective protection?

- **Legal Aid and Support:** Is legal aid provided to whistleblower?
- **Protection of Facilitators:** Are protection measures covering well facilitations, including the persons in charge with receiving whistleblowing reports?

iii. **Reporting Procedures and Channels**

- **Internal Channels:** Are there cases of good practices identified in establishing internal channels?
- **External Channels:** Are the national authorities managing external reporting provided with enough resources, independence, and authority to constitute and encourage good practices?
- **Public Disclosure**: Are rules for public disclosure formulated in a way that is not restring the whistleblowers liberty to access them if they do not trust internal or external channels?
- **Anonymous Reporting**: Are systems for anonymous reports well implemented to allow truly and full anonymity?
- **Accessibility**: Are procedures user-friendly, available in multiple formats (hotlines, online portals, physical submissions), and accessible for people with disabilities?

iv. **Cooperation with Civil Society and Social Partners**

- **NGO Involvement:** Are civil society organizations engaged in raising awareness, providing support services, and monitoring the system?
- **Trade Union Role**: Are trade unions empowered to support members in reporting and to intervene against retaliation?
- **Advisory Platforms**: Are multi-stakeholder advisory councils (including NGOs, journalists, academics) to review and improve the functioning of whistleblower protection frameworks?
- **Awareness and Training**: Are public authorities engaged in joint campaigns with NGOs and professional associations to inform the public, workers, and employers about rights and procedures and to destigmatize whistleblowing and promote it as an act of civic responsibility?

v. **Culture, Awareness, and Preventive Measures**

- **Organizational Culture:** Are there good practice cases of promotion of integrity and "speak-up" culture within organizations, including leadership commitment and non-retaliation pledges?
- **Training**: Is there good practice of training for HR managers, compliance officers, investigators, and judges on handling whistleblowing cases?

8.3. References

Council of Europe. (2014). Recommendation CM/Rec(2014)7 of the Committee of Ministers to Member States on the Protection of Whistleblowers.

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

ISO. (2021). ISO 37002:2021 Whistleblowing Management Systems – Guidelines. Geneva: International Organization for Standardization.

OECD. (2016). Committing to Effective Whistleblower Protection. Paris: OECD Publishing.

OECD (2025). Good Practice Guidance on internal controls, ethics and compliance Paris: OECD Publishing.

Transparency International. (2013). International Principles for Whistleblower Legislation. Berlin: Transparency International Secretariat.

Transparency International. (2017). The Business Case for 'Speaking Up': how Internal Reporting Mechanisms Strengthen Private-Sector Organisations. Berlin: Transparency International Secretariat.

Transparency International. (2021). Are EU Governments Taking Whistleblower Protection Seriously? Progress Report on Transposition of the EU Directive. Berlin: Transparency International.

Transparency International. (2025). Monitoring Internal Whistleblowing Systems. Berlin: Transparency International.

United Nations. (2004). United Nations Convention against Corruption (UNCAC). New York: United Nations.

National Legislation and Institutional Frameworks

Bulgaria. (2023). Law on the Protection of Persons Reporting or Publicly Disclosing Information on Violations.

Czech Republic. (2023). Act on the Protection of Whistleblowers (Zákon o ochraně oznamovatelů).

France. (2016, as amended 2022). Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (Sapin II).

France. (2022). Loi n° 2022-401 visant à améliorer la protection des lanceurs d'alerte.

Greece. (2022). Law 4990/2022 on the Protection of Persons Reporting Violations of Union Law.

Luxembourg. (2023). Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 relative à la protection des personnes qui signalent des violations du droit de l'Union.

Romania. (2007). Law No. 144/2007 on the Establishment, Organisation and Functioning of the National Integrity Agency, as amended.

Romania. (2022). Law No. 361/2022 on the Protection of Whistleblowers in the Public Interest, as amended.

Spain. (2023). Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Sweden. (2021). Act (2021:890) on the Protection of Persons Reporting Irregularities.