Open the whistle

Whistleblowing Integrity

TOOLKIT

Co-funded by
the European Union

The Project “Open the Whistle: Protecting whistleblowers through transparency, cooperation and Open Government strategies” (OPWHI) is a project Co-Funded by the European Union (Project: 101140801 — Call: CERV-2023-CHAR-LITI-WHISTLE) that seeks to create an environment that supports protected reporting of breaches of Union law and other infringements, promoting a culture where whistleblowers can safely speak up.

2025 Transparency International España
ISBN: 978-84-09-73335-4

Graphic concept and cover pages: Alessia Riolo
Design and layout: Álvaro Arribas Jiménez

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

PROJECT PARTNERS

Libera - Associatons Names and Numbers Against Mafias (Libera - Associazioni e numeri contro le mafie) - is a network of civil society organizations committed to combating corruption and organised crime while opposing those who enable them, with the aim of promoting social justice and democracy. Founded in Italy in 1995, the network currently includes 278 local groups and 80 international organizations across 35 countries in Europe, the Western Balkans, Africa, and Latin America. Since 2016, it has been actively involved in protecting whistleblowers, particularly through Linea Libera, a listening and support service for potential whistleblowers from both the public and private sectors. Libera closely collaborates with the Italian National Anti-Corruption Authority (ANAC), public administrations, other CSOs and local communities to better support potential whistleblowers and to promote shared initiatives against corruption.

University of Pisa (Università di Pisa - UNIPI) – Since 2010 the Department of Political Science of the Università di Pisa organises the Master Programme in "Analysis, Prevention and Fight against Organised Crime and Corruption", which has trained more than two hundred students from all Italy and abroad on anti corruption and anti-mafia. Moreover, UNIPI runs the Observatory on Political Corruption.

Transparency International Spain (Transparency International España - TI:E) - Through public policy monitoring, campaigns and research, TI-E advocates for greater transparency and integrity in all areas of public life. Regarding the public sector, through dialogue, collective action, training and joint work with public administrations and the government, TI-E seeks to promote and foster a culture of transparency, integrity, speak-up and accountability in the Spanish public sector. Thus, it actively participates in the design, development, monitoring and evaluation of public policies on corruption prevention and Open Government, promotes the realisation of the principles and commitments of Open Government in Spain and is part of several whistleblowing groups.

Centre for the study of Democracy (CSD - Център за изследване на демокрацията) - Founded in late 1989, it is an interdisciplinary research-oriented think-tank with regional focus on Europe and the Western Balkan countries. CSD has published a number of reports, handbooks and guides on human rights protection, rule of law and anti-corruption. The organisation is actively involved in improving whistleblowing policies and culture as a regional anti-corruption actor and member of the South East Europe Coalition on Whistleblower Protection (SECWP). CSD actively advocates for the transposition of the EU Whistleblowing Directive 2019/1937/EU in Bulgaria. Its experts participated in the Ministry of Justice working group, which drafted the law transposing the Directive 2019/1937/EU, and provided comments on all draft laws submitted to the parliament.

The Italian National Anti-Corruption Authority (Autorità Nazionale Anticorruzione - ANAC) - It is the authority in charge of receiving and investigating Whistleblowing reports of offences and of retaliatory measures taken against whistleblowers. ANAC protects the confidentiality of the identity of the whistleblower and the content of the reports and, through the use of an IT platform's encryption system, can communicate anonymously with the whistleblower. ANAC's sanctioning power includes cases of retaliation, cases of inaction by responsible officers who have not carried out any verification and analysis of the report received, and cases of absence of a system for managing reports.

Antifraud Office of Catalonia (Oficina Antifrau de Catalunya - OAC).- It is a public- law institution created by law 14/2008, on November 5th. Its purpose is to prevent and investigate cases of illegal use or allocation of public funds or any other irregular appropriation arising from acts involving conflict of interests or the use for private benefit of information deriving from the inherent functions of civil servants. It also provides advice and making recommendations for the adoption of measures against corruption, fraudulent practices and behaviour that is in breach of integrity and transparency. The Office has also been entrusted with the functions that the State Law 2/2023, transposing the Directive 1937/2019/EU assigns to the Independent Authority of Protection of Reporting persons to OAC and the Office can also exercise its sanctioning powers regarding the infringements of the Law 2/2023, which regulated the protection of persons who inform on regulatory breaches and fight against corruption.

Commission for Personal Data Protection (CPDP - Комисия за защита на личните данни) – the Bulgarian Commission for Personal Data Protection is the national authority in charge of receiving whistleblowing reports. CPDP applies protection to the individuals taking into account the conditions, procedure and measures for protection of whistleblowers in the public and private sectors who report information, or publicly disclose information about Bulgarian legislation, or acts of the European Union, that endanger or damage the public interest and the European Union law, as well as the terms and conditions for submitting and considering such information or publicly disclosed information.

ACKNOWLEDGEMENTS

The project partners would like to acknowledge the invaluable inputs of all the experts, youth, representatives of the project partners and all those who participated in the development of this guide.

Working group

ANAC	Giulia Cossu Giovanni Paolo Sellitto Valentina Tomassi
CSD	Maria Yordanova Dimitar Markov
CPDP	Hristo Alaminov Yoan Angelov Atanaska Georgieva Kristina Radkova-Staneva Katya Stanimirova Radostina Takova Desislava Toshkova-Nikolova
Libera	Leonardo Ferrante Elisa Orlando Carlotta Bartolucci
OAC	Elisenda Escoda Marisa Miralles Òscar Roca Jordi Tres
TI-E	David Martínez García Ailén Rubio Arrieta Camila Cella Andrea Rivera
UNIPI	Alberto Vannucci Francesca Rispoli Martina Cataldo Eugenio Pizzimenti

SCIENTIFIC COMMITTEE

Laura Valli, ANAC
Massimiliano Andretta, UNIPI
Roberta Bracciale, UNIPI
Valentina Maria Donini, Scuola Nazionale dell'Amministrazione (SNA)
Ventsislav Karadjov, CPDP
Delyana Doseva, CSD
Elisabet Martínez, OAC
Silvina Bacigalupo Saggese, TI-E
Ramón Ragués i Vallès, UPF

TABLE OF CONTENTS

INTRODUCTION AND STRUCTURE OF THE TOOLKIT

WHAT IS THE PURPOSE OF THIS TOOLKIT?

This toolkit arises from the **knowledge**, research and hard work of Authorities, Academia and Civil Society Organisations from **Italy**, **Bulgaria** and **Spain**. It aims to provide theoretical knowledge and practical guidance to establish a new narrative and a robust protection model for whistleblowers. There is a need to **guarantee a safe and supportive environment** for whistleblowers and **facilitate effective reporting of misconduct.**

This toolkit explores **five essential aspects of whistleblowing**, structured into five chapters, offering fresh insights and practical recommendations to implement **best practices and foster a new narrative** around whistleblowing:

A. Chapter 1 → Transparency and communication of reporting systems;
B. Chapter 2 → Proper investigation and management within internal whistleblower systems;
C. Chapter 3 → Data protection;
D. Chapter 4 → Protection and support of whistleblowers;
E. Chapter 5 → Measurement and evaluation of system effectiveness and assessment of the establishment of a whistleblowing culture.

By equipping **different stakeholders** with the appropriate tools and knowledge, this toolkit:

A. provides information about **standardized reporting mechanisms, confidentiality measures, and anti-retaliation policies**;
B. addresses challenges within national whistleblowing legislation and issues arising from the **transposition of the European Directive 2019/1937/EU**, striving to bridge existing gaps or, where not possible, acknowledging unresolved questions;
C. delivers a **dynamic analysis**, examining the evolution of responses to the Directive 2019/1937/EU and identifying **ongoing challenges six years post-implementation**;
D. offers concrete **suggestions based on lessons learned during this period**, aiming to inform future improvements.

Moreover, the toolkit recommends **best practices to promote a culture of transparency**, accountability, and ethical responsibility, ultimately strengthening institutions and increasing public trust.

THIS TOOLKIT IS NOT:

A. a handbook: It does not provide **in-depth analyses of the Directive (EU) 2019/1937** or comprehensive **country-specific assessments**. Nor does it serve as a definitive reference for evaluating compliance through scoring;

B. a single-perspective **document**: It does not examine whistleblowing solely from a legal, political, or economic viewpoint. Instead, **it integrates multiple disciplines and approaches** to provide a comprehensive understanding, recognising the multifaceted **nature of whistleblowing**;

C. a historical or theoretical analysis: It avoids delving into the **history or theoretical foundations of whistleblowing**, instead focusing on **practical insights** and actionable recommendations;

D. one-sided: It does not concentrate solely on system functionality or exclusively on whistleblower protection; rather, it recognises **the importance of both perspectives** and seeks to harmonise them.

FOCUSES ON TWO CROSS-CUTTING APPROACHES: OPEN GOVERNMENT AND GENDER

Throughout the chapters, the toolkit incorporates two fundamental approaches: **Open Government** and **gender-based approaches:**

A. the **Gender-based approach** aims to **raise awareness** about the importance of developing accessible, inclusive, and **gender-sensitive whistleblowing systems** for effective and comprehensive reporting and protection. In recent years, there has been a growing recognition of how corruption can disproportionately impact women, men, and other gender identities, highlighting the need for gender-sensitive whistleblowing mechanisms. It helps to **address gaps in legal protections and policies** that tend to be gender-blind and often overlook diversity, equality, and non-discrimination considerations. In this context, the idea is to **provide both theoretical and practical tools** to all stakeholders involved in whistleblowing, facilitating the effective integration of a gender-based approach;

B. the **Open Government approach** aims to formulate recommendations **to address whistleblowing challenges** based on Open Government core principles, such as **transparency, accountability, participation, and inclusion**. In other words, all the actions that civil society and institutions can undertake collectively and collaboratively to foster whistleblowing and protect whistleblowers. If your country is a member of the Open Government Partnership (OGP), the authors suggest making any such commitment part of the National Action Plan cycles[1], or part of the Open Gov Challenge[2], which allows for ambitious reform commitments to be made and recognized outside of the regular Action Plan cycle. This way, it will be easier to **establish a transparent relationship with all relevant stakeholders, co-create solutions and better monitor their implementation and impact**.

[1] In this regard see: https://www.opengovpartnership.org/process/action-plan-cycle/

[2] In this regard see: https://www.opengovpartnership.org/the-open-gov-challenge/open-government-challenge-areas/

WHY DOES WHISTLEBLOWING MATTER? THE NEED OF MAKING IT AN ESSENTIAL AND SYSTEMIC COMPONENT OF SOCIETY

Whistleblowing is a term which carries multiple meanings and nuances. Broadly defined, it is a "**form of reporting**" that plays a crucial role in ensuring accountability, exposing malpractice and corruption, bringing hidden wrongdoing to light, and preventing harm. Whistleblowers often witness wrongdoing and act in the public interest to prevent harm. They are entitled to fair treatment, respect, and **protection** from retaliation. However, for whistleblowing to be truly effective, it **must be integrated** as an **essential and systemic component** within workplaces and society.

Strong legal protections, clear reporting mechanisms, and a culture that encourages **ethical responsibility** are crucial in empowering individuals to speak up without fear of retaliation. Currently, behavioural norms in organisations and society can discourage individuals from speaking out about crimes or ethical violations: the need to adapt, the concept of the whistleblower **as a spy or a traitor**, and the idea that whistleblowing is an "***extrema ratio***" which requires tremendous legal efforts prevail. This is problematic because, instead of being seen as a structural element of any organisation, it is still viewed as an **extraordinary measure that requires exceptional interventions.** By institutionalizing whistleblowing as a fundamental practice, we create a safer, more transparent, and responsible environment for all.

TWO DIFFERENT BUT COMPLEMENTARY PERSPECTIVES

This document strives to balance **two perspective**s:

A. The "**whistleblowing-centered**" approach, represented by competent authorities concerned with the system's functioning.
B. The "**whistleblower-oriented**" approach, adopted by civil society organisations that care about the individual who reports, intends to report, or experiences the effects of a report, ensures their life plans are preserved.

A BRIEF HISTORY OF THE EUROPEAN DIRECTIVE 2019/1937/EU AND ITS TRANSPOSITION

In 2016, the European Commission stated that **there was no legal basis** for a whistleblowing Directive (EU) 2019/1937, however there was a need for an harmonized EU legislation on whistleblower protection. Only in 2019, in response to a series of **high-profile scandals** (e.g., LuxLeaks, Panama Papers), the EU Whistleblowing Directive (EU) 2019/1937 was adopted by the European Parliament and the Council. Its purpose was to establish a **minimum standard** for **whistleblower protection across the EU** Member States, ensuring that individuals who reported breaches of EU law were safeguarded **against retaliation**. EU Member States were given until **17**

December 2021 to transpose the Directive (EU) 2019/1937 into national law. As of 2024, most Member States have **incorporated the Directive (EU) 2019/1937 into their legal** systems, though some **faced challenges** in ensuring full compliance. National legislation differs widely regarding the conditions under which whistleblowers are protected, as well as their legal basis across countries.

WHISTLEBLOWING IN ITALY

In **Italy**, whistleblowing regulations existed before the Directive (EU) 2019/1937, with initial measures introduced in 2012 and later expanded in 2017. Law 190/2012 was the first law in Italy to introduce specific protections for whistleblowers, although it was limited to the public sector. This law allowed public employees to report misconduct they became aware of in their workplace without facing retaliation. However, the protections were weak: the regulation merely prohibited disciplinary sanctions against whistleblowers but did not provide a real protection system or clear mechanisms to ensure the confidentiality of reports. Additionally, there were no safeguards for private sector employees. In 2017, Law 179 strengthened the framework by introducing broader protections in both the public and private sectors. It established measures to guarantee the confidentiality of whistleblowers and imposed sanctions on those who attempted to retaliate against them. Furthermore, it required private companies meeting certain criteria to implement internal reporting channels.

Finally, in coherence with the Directive (EU) 2019/1937,the new whistleblowing law (Legislative Decree no. 24/2023) requires public and private entities with more than 50 employees to establish internal reporting channels that ensure confidentiality. Reports can be made to ANAC (the external channel) if internal channels are unreliable, ineffective, or if the violation poses an imminent public risk. A recognition of third sector organisations that support whistleblowers before and after reporting has been introduced by the law.The law aims to enhance safeguards against retaliation and strengthen reporting mechanisms, extending this protection beyond employees to freelancers, volunteers, trainees, shareholders, and facilitators.

WHISTLEBLOWING IN BULGARIA

Before the adoption of the Directive (EU) 2019/1937, **Bulgaria** had scattered provisions related to whistleblower protection across various laws. The Protection Against Discrimination Act prohibited retaliation against individuals filing discrimination complaints, while the Administrative Procedure Code offered general safeguards for those reporting abuse of power or corruption. Several bodies were involved in handling such reports, including the Chief Inspectorate of the Council of Ministers, ministry inspectorates, and the Anti-Corruption Commission, which served as the central authority for receiving reports of corruption and conflicts of interest.

Additionally, some public institutions and private companies - particularly those operating internationally or in regulated sectors - had already developed internal reporting mechanisms.

This fragmented framework helped ease the transposition of the Directive (EU) 2019/1937 into national law. In 2023, Bulgaria adopted the Protection of Persons Reporting or Publicly Disclosing Information on Breaches Act, which came into force on 4 May 2023. The Act mandates that public and private sector employers with 50 or more employees establish internal reporting channels, with the obligation for private employers with 50–249 employees starting on 17 December 2023. The Commission for Personal Data Protection (CPDP), designated as the central authority for external reporting, has since taken important steps to implement and enforce the legislation.

WHISTLEBLOWING IN SPAIN

Under the Criminal Procedure Act (*Ley de Enjuiciamiento Criminal* or LECrim) established in 1882, persons in Spain who witness crimes are legally obliged to report them, with penalties for non-compliance. This duty extends to "witnesses of reference" (Article 264 of the LECrim) and to certain professions, such as public authorities, who face more severe penalties for failing to report crimes (Article 262 LECrim and 408 of the Spanish Criminal Code).

On the other hand, the 2015 reform of the Spanish Criminal Code introduced the requirement that compliance programmes must include an obligation to report "possible risks and violations to the body responsible for overseeing the operation and enforcement of the prevention model" (Article 31 bis 5.4). Although the Criminal Code does not include this as an obligation, in the event of a criminal process, those entities wishing to obtain an exemption or mitigation of their liability must have internal whistleblowing channels, which in practice has meant that in Spain many private entities (especially big companies) adopted these mechanisms before the adoption of Directive 2019/1937/EU, each entity developing its own whistleblower protection policies and procedures.In the public sector, there were also some regulatory manifestations at the regional level prior to the Directive (EU) 2019/1937, for example with the Law 11/2016, of 28 November, which creates the Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community, which must establish confidential channels that guarantee strict confidentiality for the formulation of reports when the complainant invokes the application of the statute regulated in this Law.

However, **Spain** lacked widespread and consistent protection for whistleblowers until the transposition of Directive (EU) 2019/1937, effected through the *Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory violations and the fight against corruption*.

Transparency and communication of reporting systems

Chapter 1

Open the whistle

TRANSPARENCY AND COMMUNICATION OF REPORTING SYSTEMS

CHAPTER 1

1.1 WHISTLEBLOWING SYSTEM : THE NEED FOR CLEAR GUIDANCE

Trust[3] in the system is a key factor for any whistleblower. Lack of information about the available channels and the system can have a negative impact on trust, as trust cannot be built solely on the existence of the channel—a supportive and protected environment is essential for reporting.

The absence of clear guidelines may lead to misinformation and mistrust, discouraging whistleblowers and hindering the creation of a safe space for reporting breaches. Therefore, to **increase awareness and trust**, it is necessary to **provide information**, at a minimum, on:

A. Who can or should report
B. How to report
C. When to report
D. To whom to report
E. How the reporting person is protected
F. What rights the accused person has
G. How the reporting process works
H. The security measures in place
I. How to ensure that the reporting system is gender-sensitive

According to a public consultation in 2017, **only 15% of citizens were aware** of existing whistleblower protection rules, and **49% did not know where to report corruption** (EU 2018)[4]. Similarly, some studies[5] demonstrate that establishing a solid foundation for a whistleblowing program – i.e., defining clear operational procedures or guidelines for both officers and staff members of authorities and for whistleblowers - is a successful practice for

[3] According to Binikos (2008), trust in one's organisation and management were positively associated with intentions to blow the whistle across 16 studies (among others: Attree, 2007; Brennan and Kelly, 2007; Binikos, 2008; Curtis and Taylor, 2009; Seifert et al., 2014; etc.).

[4] In this regard see: https://ec.europa.eu/newsroom/just/items/54254/en

[5] Australian Securities and Investment Commission, 2023; among others.

properly handling disclosures. Because whistleblowing is a complex process with personal and psychological implications, organisational and cultural measures are required to support the implementation of the law, while also considering the cultural attitudes toward whistleblowers[6].

Despite the Directive (EU) 2019/1937 clearly **defining rights and principles**, it does not contain clear and detailed provisions regarding the information and transparency that all obliged entities (Article 8) must provide about their **channels and systems.** Article 13 of the Directive (EU) 2019/1937 establishes a general obligation for competent authorities, while Article 9.1 imposes a requirement for obliged entities to inform about "procedures for reporting externally to competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union" (Art 9.1.(g)).

As a result, **potential whistleblowers** and other citizens interested in reporting may not be adequately informed about the available channels, the reporting system, the procedures and authorities involved, rights, deadlines, technical information, protective measures and IT security system features.

In Spain, *Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory violations and the fight against corruption*[7], dedicates Title IV to regulating the information that must be provided by both entities and competent authorities on the internal and external channels. The law expressly stipulates that this information **must be visible on websites** or electronic platforms, in a separate and easily accessible section. It also requires that all entities required to have an internal channel, in both public and private sectors, must maintain a logbook of received complaints and any internal investigations resulting from them. However, this logbook is not public and is only accessible to judicial authorities.

Article 25 of Law 2/23 explicitly states that: "**entities included within the scope of application of the Law** "shall provide adequate information in a clear and easily accessible form, on the use of any internal information channel they have implemented, as well as on the essential principles of the management procedure. In the event of having a website, such information shall be included on the home page, in a separate and easily identifiable section."

[6] Teichmann et al., 2022.

[7] Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory violations and the fight against corruption https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513

However, the law does not specify the essential content of what the entities must necessarily inform to the public about their reporting systems in their websites[8].

In **Italy**, all public and private entities are required **to provide clear information on the channel,** procedures and prerequisites for making internal reports, as well as on the channel, procedures and prerequisites for making external reports[9].

This information **must be easily visible in the workplace** and accessible to individuals with a legal relationship with the entity. If the entity has a website, the information must be published in a dedicated section. Additionally, the law[10] states that as the **competent authority** for managing the external reporting channel, ANAC must publish information such as:

A. protection measures for whistleblowers;

B. contact details, such as the telephone number of the office that manages the reports, indicating whether or not the telephone conversations are recorded, the postal address and the email address, both ordinary and certified;

C. confidentiality rules applicable to external and internal reports.

In **Bulgaria**, the Protection of Persons Reporting or Publicly Disclosing Information on Breaches Act of May 4, 23, in line with the Directive 2019/1937/EU, states that "(...) Obliged entities shall provide clear and easily accessible information on the conditions and procedures for submitting whistleblowing reports. The information shall be made available on the websites of the obliged entities as well as in prominent places in offices and workplaces"[11](Article 12(4))."

Although this obligation has been **formally implemented**, **there is no assessment of its effectiveness**.

Meaningful transparency and effective communication are not minor issues; they are essential for ensuring that whistleblowing systems function properly. Individuals cannot make informed decisions on whether, when, and how to report if they are not adequately informed in advance about their **fundamental rights and obligations**, the **essential principles** and

---

[8] For the authorities mentioned in Article 24, the Law sheds a little more light by establishing that they shall publish, in a separate, easily identifiable and accessible section of their electronic site, at least, the following information: "(a) the conditions for eligibility for protection under this law; b) the contact details for the external information channels provided for in Title III, in particular, the e-mail and postal addresses and telephone numbers associated with such channels, indicating whether telephone conversations are recorded; (c) the management procedures, including the manner in which the competent authority may request the informant to clarify the information communicated or to provide additional information, the time limit for replying to the informant, if any, and the type and content of such reply; d) the confidentiality regime applicable to communications and, in particular, information on the processing of personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December and Title VII of this law. e) remedies and procedures for protection against retaliation, and the availability of confidential advice. In particular, the conditions for exemption from liability and mitigation of the penalty referred to in Article 40 shall be provided for and (f) the contact details of the Independent Whistleblower Protection Authority, I.W.P.A. or of the competent authority or body concerned."

[9] Art.5.1 Legislative Decree, March 10 2023, n.24

[10] Art. 9, Legislative Decree 24/2023, transposing Directive 2019/1937/EU

[11] Protection of Persons Reporting or Publicly Disclosing Information on Breaches Act, Bulgaria, May 4, 2023, Article 12(4)

steps of the reporting process, and basic details on the nature and operation of reporting channels within an organisation or public body[12].

Additionally, authorities and oversight bodies can **more easily supervise** obligated parties by monitoring their compliance through periodic reviews of transparency measures and the active promotion of accessible reporting channels.

From the review of the Directive (EU) 2019/1937. Recitals num. 59 and 75, the article 25 of the Spanish Law 2/23, the article 12 of Bulgaria's Whistleblower Protection Act, article 5.1 and 9.1 of the Italian Legislative Decree 24/2023, and considering the aforementioned, it follows that **two basic conditions** must be met to ensure adequate and comprehensive transparency in information systems and channels so that they can effectively fulfil their mission: one related to **content** and another related to **form**.

1.2 TRANSPARENCY REGARDING THE RIGHTS AND GUARANTEES OF WHISTLEBLOWERS AND AFFECTED OR ACCUSED PERSONS

Regarding the substantive aspect, all obligated parties must provide **clear, complete, updated, and structured information**, at least, on the following areas:

1.2.1 TRANSPARENCY REGARDING THE RIGHTS AND GUARANTEES OF WHISTLEBLOWERS AND AFFECTED OR ACCUSED PERSONS

It is necessary to include a specific section (both on the website and on the intranet, if applicable) with a complete list of the **rights of both the whistleblowers** and the persons concerned, as well as third parties (for example someone that is mentioned in the report, witnesses, worker's representatives/unions, co-workers of the whistleblower) if applicable.

As for potential whistleblowers, it should include at least the:

A. confidentiality protection of the reporting persons and of the content of the report;
B. non-retaliation[13] in the terms established in the Directive (EU) 2019/1937 and in the national laws;
C. clear information on the bodies managing the report;
D. right to receive a reasoned response on the decision to archive, dismiss, or not proceed with the report;

[12] The European legislator has been very clear in this regard: "all individuals who are considering reporting breaches of Union law should be able to make an informed decision about whether, when, and how to report. Legal entities in the private and public sectors that have internal reporting procedures should provide information about these procedures, as well as about external reporting procedures to competent authorities. It is essential that this information be clear and easily accessible, including, as far as possible, to individuals who are not employees in contact with the entity due to their professional activities, such as service providers, distributors, suppliers, and business partners. For example, such information could be displayed in a visible place accessible to all these individuals and on the entity's website, and it could also be included in ethics and integrity training courses and seminars." (Recital 59 of Directive 2019/1937/EU). Furthermore, in a subsequent recital, it is reiterated that "all information regarding reports must be transparent, easily understandable, and reliable in order to encourage reporting rather than obstruct it."(Recital 75 of Directive 2019/1937/EU).

[13] According to one of the experts interviewed, it is important to report on how retaliation is prevented, how whistleblower protection is guaranteed and outline the specific processes ensuring this.

E. personal data protection[14];
F. acknowledgment of receipt and diligent follow-up of reports;
G. timely and appropriate resolution notification[15];
H. a fair, independent, and impartial investigation;
I. legal advice, legal and psychological support, or support from workers' representatives. (if required by law);
J. right to good administration, under Article 41 of the Charter of Fundamental Rights of the European Union (especially relevant for public sector obliged entities);
K. psychological support (if required by law or offered by the entity);
L. financial support (if required by law or offered by the entity).

As for the accused/concerned persons, it is necessary to include at least:

A. Presumption of innocence.
B. Identity/Confidentiality protection.
C. Right to be heard.
D. Access to the investigation file.
E. Due process rights.
F. Right to present evidence.
G. Legal defense and worker representation.
H. Right to know the instructing body and to an impartial judge.
I. Personal data protection rights.

Finally, it is also important to include the r**ights and guarantees of third parties** potentially related, affected, or named in a report (witnesses, persons named in a report, family members, or persons who may suffer some type of harm or retaliation as a result of the report, as well as those providing legal, labor, or psychological support).

Facilitators and information centres should also be included (**see Chapter 4** for further details on this point).

Ch. 4>

1.2.2 Material scope for reporting

Transparency regarding the material scope. It is advisable to indicate which areas can or should be reported, as well as the applicable regulations[16]. Additionally, it is recommended that internal and external channels provide a point of contact for inquiries and a Frequently Asked Questions section.

[14] Including, but not limited to: The right to be informed about the identity of the data controller, the purpose of the processing and the possibility to exercise the rights set out in Articles 15 to 22 of RGPD and the right to erasure of data after three months, unless disciplinary or criminal disciplinary or criminal proceedings.

[15] In this regard, see. Indicator No. 94 of the TRAC-SPAIN 2022 Report (p. 159).

[16] Indeed, another one of our interviewees highlighted that it is crucial to be informed about the legal framework and the risk of litigation.

GENDER BOX

Stakeholders across all sectors and countries emphasize the need to address **cross-sectoral inequalities**, including gender, intersectional and diversity issues. The nature of the misconduct reported and the risk associated with it significantly impact the decision to report.

Ch. 4>

Cases of gender-based abuses of power, such as sexual harassment or sextortion, are often linked to a higher risk of retaliation (see box in **Chapter 4**), which can discourage victims from blowing the whistle. In some cases, victims may be unsure whether such misconduct falls under whistleblowing legislation. Stakeholders have recommended explicitly including these issues within whistleblowing frameworks. In Bulgaria, civil society representatives have emphasized that if gender-related issues arise in the workplace, whistleblowing legislation should address them alongside existing legal provisions against discrimination.

It is recommended to:

A. ensure that EU gender-based violence (GBV) legislation and national standards are mainstreamed into whistleblowing mechanisms to provide comprehensive protection. Expand the scope of protection to cover all potential wrongdoings, abuses, and other offenses, including sexual harassment and sextortion. The whistleblowing legal framework should address gender-based discrimination in the workplace, in addition to the applicable legal provisions against discrimination and provide support and protection to victims of sextortion and sexual harassment within whistleblowing legislation;

B. future international, national and subnational regulatory frameworks should reinforce measures to establish tailored protection mechanisms for women whistleblowers and other vulnerable groups, ensuring that reporting channels are accessible, inclusive, and responsive to their specific needs and risks;

C. develop gender-sensitive protocols within whistleblower frameworks to specifically address cases of sexual harassment, sextortion, and other gender-based misconduct. Integrate transparency regarding the rights and safeguards of whistleblowers with an emphasis on gender-sensitive communication and the inclusion of marginalized groups. Clear communication about rights, guarantees, and the authorities responsible for handling reports ensures that whistleblowers feel confident in the system and understand their protections. This includes clear, accessible guidelines on the procedures, support options, and legal protections against retaliation;

D. coordinate with other services for more effective handling and to prevent impunity, avoiding the assumption that sextortion cases can be better addressed by other services or complaint mechanisms, such as those dealing with sexual violence;

E. provide concrete examples of gender-based cases to enhance clarity and accessibility for potential whistleblowers, reinforcing their rights and available protections;

F. each person should be informed of their right to report or disclose wrongdoing directly to the relevant specialized authorities, such as the police, prosecution, or courts, particularly in cases of GBV. This ensures that the individual is aware of all available options for addressing the issue and seeking the appropriate support. Compensation settlements shouldn't exclude access to justice systems;

G. ensure that reporting platforms use clear, non-technical language and offer channels in multiple languages, including sign language and other accessible formats, to accommodate a diverse range of whistleblowers. Ensure gender-inclusive language, making gender visible when relevant, and avoiding unnecessary gender markers when not pertinent to the communication. This approach promotes clarity, inclusivity, and respect for diverse gender identities in all forms of communication;

H. consider the impact of digital access disparities, ensuring alternative offline reporting mechanisms for individuals without secure internet access, promoting inclusivity for all users regardless of their digital access capabilities.

WHAT HAPPENS IN THE NATIONALWHISTLEBLOWING LEGISLATION?

ITALY

The concept of **sexual harassment** is relevant from an **anti-discrimination law** perspective. In 2006, Italy adopted the so-called *Code for Equal Opportunities for Men and Women (Legislative Decree No 198/2006)*, which contains a definition of sexual harassment. In the absence of whistleblowing legislation covering sexual harassment at work, it is left to the willingness of employers to implement internal procedures that allow employees to report harassment or bullying.

SPAIN

The Whistleblowing Law 2/2023 (*Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption*) does not explicitly address gender-based violence (GBV). However, it operates within a recognized normative framework for the prevention of gender-based violence, equality, and non-discrimination, as well as national plans and specific public policies on this topic. Three key points are worth mentioning:

A. the material scope of the law extends beyond European requirements, applying to both criminal and administrative offenses, including violations of national law. This allows reporting mechanisms to address all GBV offences;

B. even though the law does not preclude incorporating this issue into regulations or protocols, gender-based protection is fully compatible with the whistleblowing legal framework. Not only should both be integrated with the GBV legal framework, but the whistleblowing law also includes protections for workers who report any form of abuse or violations of their dignity, health, and safety. Therefore, the protection and safeguards must cover any violation of physical or psychological integrity, including any form of gender discrimination or sexual abuse;

C. the Royal Decree establishing the Independent Authority for the Protection of Whistleblowers (A.A.I.) mandates gender-balanced representation within the Consultative Commission, setting a valuable precedent for other national or local authorities.

BULGARIA

Sexual harassment is not covered by the national Whistleblowing Act. However, there is a view that if the harassment occurs in a work context and threatens the public interest, the report could be considered whistleblowing, and the whistleblower may be afforded due protection.

Several experts interviewed have pointed out that some transposition laws have left ambiguities, inequalities or unprotected areas regarding several aspects, including what can or cannot be reported[17]. These unprotected areas may discourage potential whistleblowers. For example, according to Law 2/2023 in Spain, whistleblowers who report irregularities involving a minor offense in matters other than those contained in the Directive (EU) 2019/1937 would not be entitled to protection under the law.

1.2.3 Transparency regarding the essential principles[18] of the management procedure.

Entities **must clearly define** the essential principles of the whistleblowing procedure, including its purpose, management, and compliance framework. For example, in Spain, these principles must be explicitly reflected in the Internal Information System Policy[19]. Providing adequate information in this section **is crucial to inform** about why the reporting channel exists, encourage proper use of the system, and deter improper use.

A. regarding **security**, it is essential to inform about the IT characteristics of the server or platform and the information security measures in place to ensure a secure digital environment for whistleblowers, namely: encryption, pseudonymization, encoding, black boxes, access control, secure connection protocols, dual-step authentication, validation rules, appropriate descriptions of firewalls, comprehensive descriptions of the server/software characteristics, CSRF token, etc;
B. in relation to **immunity**, it is necessary to clearly and transparently inform about the scope of whistleblower protection, the conditions for accessing protection under the Law, and explicitly guarantee that there will be no reprisals against whistleblowers if the reports are funded;
C. regarding **confidentiality**, it must be clearly and simply explained how the confidentiality of the whistleblower is guaranteed, namely: assurance of the principle of minimal access and data integrity, explanation/justification of data processing, description of data handling during all phases of the process, retention time and location of the information, data and whistleblower identity protection measures, description of anonymisation and pseudonymization systems, description of control, monitoring, and segregation of whistleblower files from different files, measures to prevent re-identification; and in case the channel or a part of the process is outsourced, it is important to describe all the security measures established by the provider and the server;
D. in relation to **anonymity**, it is essential that the reporting channels are designed in such a way as to allow, if the whistleblower so wishes, to submit communications completely anonymously, without compromising his or her identity at any stage of the process. However, it should be stressed that the Directive (EU) 2019/1937 does not

[17] For example in Spain, the Law 2/2023 only protects and recognizes rights to those who report only on: a) criminal offenses (crimes), b) serious or very serious administrative offenses and/or c) infringements of European Union law and affecting the financial interests of the European Union; excluding for example minor offenses or cases that could help prevent more serious crimes. Some of the experts also raised the question as to whether reports of maladministration would be accepted.

[18] Art. 5.2. h) Spanish Law 2/23, art 13 Bulgarian Law, art. 4, 5, 7, 8 of the Italian Legislative Decree 24/2023, transposing the Directive 2019/1937/EU. In this regard, see Chapter XXX.

[19] In this regard, please see Chapter II.

recognize anonymity as a protected right per se but leaves it to the Member States to admit and process anonymous reports according to their national legislation. Therefore, although anonymity is not directly guaranteed by the Directive (EU) 2019/1937, its voluntary incorporation into reporting systems is a good practice.

If the whistleblower identifies themselves in the channel or system, **confidentiality** ensures that their identity is not revealed to unauthorized persons. Security systems (usually achieved through encryption, access controls, etc.) could be useful in keeping confidentiality protected, but internal whistleblower policies detailing the confidentiality regime and the roles of responsible persons need to be developed to ensure that the identity of whistleblowers remains protected.

Anonymity, on the other hand, should ensure that a person who wants to keep their identity secret can be sure that this is the case, therefore, in this instance, a person's identity could not be linked to their actions, displays, data or IP, protecting the lack of traceability of the whistleblower's identity (achieved, for example, through TOR systems or zero-knowledge proofs).

According to some of the stakeholders, a number of mailboxes or channels of some public institutions have been detected[20] that claim to guarantee anonymity but in practice this is not the case.

1.2.4 Receiving, managing, investigating and resolving bodies

It is important to ensure transparency regarding the **receiving body** and the **managing body** (if separate), as well as the **investigative body** and the **resolving body**. This organisational separation is crucial not only to foster greater trust in the system but also to ensure compliance with the principle of impartiality and independence in all investigative processes initiated as a result of reports.

It is also necessary to include **an explanation of the measures** in place to prevent potential **conflicts of interest** between the bodies or different departments and to provide alternative options if the person responsible for the system or any member of the intervening bodies (receiving, managing, instructing, or resolving bodies, as well as second or potential instances) are involved in the report.

1.2.5. Acknowledgment, admission, investigation and resolution dates and deadlines

1) First Stage

[20] In this regard see: https://xnet-x.net/es/proliferacion-buzones-anonimos-no-lo-son/

According to the Directive (EU) 2019/1937 (Art.9.2[21], the **acknowledgment of receipt** should be given to the whistleblower within a maximum period of seven calendar days following the receipt or registration of the report, unless doing so could jeopardize confidentiality.

2) Admission deadlines

The website or intranet should indicate the deadline for preliminary investigations, or for decision on the **admissibility of the report**[22] This assessment implies the gathering of all the necessary information, documentation, and evidence. Consequently, the entity must explicitly inform about the following aspects:

A. **maximum deadline for conducting the preliminary admissibility test** in order to avoid undue delays. This is not provided by the Directive (EU) 2019/1937, nor the Spanish Law 2/2023, Bulgarian or Italian laws, but which, for example, the timeframe granted to the Spanish Independent Authority for admitting or rejecting a report in the Law 2/2023 is "no more than ten working days from the date of registration of the communication"; this could be a good parameter to be considered depending on the characteristics and capacities of the entity, but what is recommended is that a clear time frame be publicly provided in order to avoid undue delays;

B. **maximum deadline for notifying the whistleblower about the admission for processing or filing of the report/communication**. Again, neither the Directive 2019/1937/EU nor the Spanish Law 2/2023, Bulgarian or Italian clearly regulate this aspect. For example, the Spanish Law establishes a maximum notification deadline of "five working days", but does not specify when these five days should be counted.

In our view, this **deadline should start from** the moment the preliminary admissibility test is conducted (whose maximum execution period, as indicated earlier, would be for example ten working days from the date of registration[23]), unless the report is anonymous, or the whistleblower has waived receiving notifications.

Another important aspect to consider is that, under the Spanish Law 2/23, all these report processing or filing deadlines refer exclusively to the whistleblower. Neither the Directive nor national laws specify clear notification deadlines for the affected person at this procedural stage. This raises questions about whether the affected person has the right to be notified about filing a report that does not pass the preliminary admissibility test.
From a broad reading of Article 18.2. a) 4º of the Spanish Law 2/2023, it could be inferred that such notification is unnecessary since it establishes

[21] Art. 9.2.c) of the Spanish Law 2/23, Art. 16(1) and 23(1) of the Bulgarian Law, Art.5 a) and 7.3 of the Italian Law, respectively for internal and external channels, establishing also a term of 7 days to issue a receipt of the report..

[22] In this regard, see MARTÍNEZ GARCÍA, D (2021). 'Anonymity, Pseudonymity, and Confidentiality: Towards a Comprehensive and Coherent Framework for the Protection of Whistleblowers'

[23] For example, if the admissibility test is completed on the eighth working day after the registration of the communication, the entity would have five additional working days from that moment to notify the whistleblower whether their communication is admitted, making a total of thirteen working days from the registration of the communication.

inadmissibility due to the lack of **new or significant information** compared to a previous communication "in relation to which the corresponding procedures have been concluded."

However, this is a procedurally ambiguous formula because:

A. By referring to procedures in the plural, it could involve a communication that was already filed[24] for failing the **admissibility test**, followed by a subsequent complementary report providing relevant, significant, or decisive new evidence[25]. This raises the issue of the maximum time for retaining personal data from a field report[26]. For example, under Article 32.3 of the **Spanish Law**, if the report is inadmissible due to the cause established in Article 18.2. a) 1º (lack of plausibility) and it is proven that the provided information or part of it is not true, the Law states that "it shall be immediately deleted once this circumstance is confirmed, unless such untruthfulness may constitute a criminal offense, in which case the information will be retained for the necessary period during which judicial proceedings are underway," and, in any case, no more than three months, unless the purpose of retention is to provide evidence of the system's operation[27], in which case the information must always be retained in an anonymised manner.

B. It could also refer to cases where, after it has been decreed that the affected person is not notified until the **hearing phase** due to a risk of **evidence destruction**, concealment, or alteration (Article 19.2 of Spanish Law 2/23), complementary communications (under Article 18.2.a) 4º of this Law) are made by the whistleblower including new accusations against the affected person. In such cases, barring once again a risk of evidence concealment, destruction, or alteration related to these new accusations, the affected person should be notified according to the usual procedure to avoid potential defencelessness.

3) Investigation process deadlines

Regarding **investigation deadlines**, although the **Directive and national Laws** state that the accused person is notified about a report, as well as of the facts succinctly described in it. However, it does not establish a clear timeframe for this. In this respect, we shall take into account that an obligation to inform accused persons of a report against them should be assessed against the possibility of retaliation and identification of the whistleblower. Accused persons must be informed when there is a need to defend themselves, for example in cases of alleged retaliation, but not necessarily after receiving a report.

Entities must establish these deadlines within their internal policies to ensure the protection of the accused individual's procedural rights. This includes guaranteeing the right to be adequately informed about the allegations against them, as well as any significant modifications to the

[24] Any notification regarding the filing of a report must be sufficiently reasoned.

[25] As long as these new pieces of evidence have not been obtained in violation of fundamental rights or freedoms or illegally.

[26] In this regard, see Chapter 3.

[27] Which may raise issues about an unlimited potential reopening of cases filed during the preliminary evaluation phase, raising questions related to the possible violation of the principle of non bis in idem.

scope of the investigation and the alleged facts, in accordance with Article 118.1(a) of the Spanish Criminal Procedural Code. In this regard, the Criminal Procedure Law explicitly states that "this information will be provided with sufficient detail to allow the effective exercise of the right to defense." This implies that safeguarding this right requires not merely a brief summary of the facts but a level of detail sufficient to enable an effective defense.

The authors of this guide believe that once admission for processing a report/communication is agreed upon, the same maximum notification deadline should be applied to the accused person as it is to the whistleblower (and in any case never a longer deadline): five working days following the decision to admit the report for processing, to notify the affected person that an investigation of a report by which they are accused has been admitted and initiated[28]. However, if the investigating body deems that notifying the affected person could pose a high risk of evidence concealment, destruction, or alteration by them or third parties, this information may be provided to the affected person during the hearing phase[29].

4) Judgement deadlines

Regarding judgement deadlines, it must be clearly and transparently communicated that the maximum response time[30], shall not exceed three months from the receipt of the communication, except in cases of special complexity that require an extension of up to a maximum of three additional months.

1.2.6 Applicable disciplinary regime

Transparency regarding the applicable disciplinary regime and the consequences of deliberately communicating manifestly false or misleading information should be clearly informed. As already mentioned in this Chapter, it is necessary to properly inform about the ultimate purpose of the channel and discourage its incorrect use.

To this end, it is advisable to inform those who knowingly **submit false information** — attributing false facts to another person that would, if true, **constitute an infraction, or falsely claiming to be a victim** of a non-existent infraction. In some legislations they are committing a **crime (art. 456 Spanish Criminal Code) and in others are subject to severe administrative sanctions (concrete reference to Italian Law)**; In Italy, the law provides administrative sanctions against a whistleblower who knowingly submits false reports. The entity must report this fact to the relevant authorities and act accordingly.

---

[28] All of this based on Article 118.5 of the Spanish Criminal Procedure Code (LECrim), which establishes that: “The admission of a report or complaint, and any procedural action that results in the accusation of a crime against a specific person or persons, shall be immediately brought to the attention of the allegedly responsible parties.”

[29] According to Article 19.2 of Spanish Law 2/2023, Art. 16 of the Bulgarian Law.

[30] According to Article 9.2.d) of the Spanish Law 2/23, Art. 16 (for internal channels) and Art. 23 (for the external channel) of the Bulgarian Law; and art. 5 (related to the internal channel) and 8 (related to the external channel) of the Italian Law.

1.2.7. Contact details of the external channels

The contact details of the **external official** channels[31] are: the email and postal addresses and the telephone numbers associated with these channels and, in any case, the contact details of the independent authority[32] and other competent authorities for receiving such communications, as well as the available appeal routes and procedures for protection against retaliation, along with the conditions for obtaining legal, labor, psychological, and financial advice and support (in the event they are foreseen).

OPEN GOV BOX

Stakeholders across all sectors suggest that **a collaborative approach** involving civil society organisations (CSOs) and public authorities **can enhance information pages and reporting systems for clarity while ensuring a whistleblower-oriented perspective**. This means making reporting procedures accessible and easy to understand.

In line with this, civil society organisations suggest simple yet effective strategies to improve content usability and increase trust in reporting channels:

A. Use plain language that is easy to understand, avoiding technical or legal jargon.
B. Provide practical examples whenever possible.
C. Repeat key reporting instructions throughout the reporting process, including on the information page and within the reporting channel.
D. In the reporting platform or form, request the subject of the report first and only ask for the reporting person's name at the end.

To improve reporting systems and information pages, **public consultations open to all stakeholders can help refine content and usability** while encouraging reporting. The competent authority should lead such consultations, setting an example for other obligated entities to replicate these efforts or promote their own public consultations.

Best practices in Open Government (OG) include **providing clear information on public authorities' websites about whistleblower support and advisory services** managed by institutions (e.g., Ombudsperson's Office) and CSOs. This provision is not explicitly covered under Directive. However, since it only sets minimum standards, EU countries that wish to go beyond its requirements and include this provision in their national laws or regulations are strongly encouraged to do so.

For example, **Italy's 5th National Action Plan (5NAP) for Open Government (2021-2023)**[33], **focused on strengthening collaboration between institutional and civil society actors to support whistleblowers and raise awareness.**

Key outcomes included:

A. **Fostering visibility and accessibility to support services of CSOs**: The National Anti-Corruption Authority (ANAC) led a task force involving civil society and public

[31] Title III of Spanish Law 2/23, Art. 21 of the Bulgarian Law, and art. 9 (for the external channel, managed by ANAC) of the Italian Law,

[32] In Spain the Independent Authority for Whistleblower Protection (A.A.I.), In Italy the Anti-Corruption National Authority (ANAC), in Bulgaria the Commission for Personal Data Protection.

[33] In this regard see: https://www.opengovpartnership.org/members/italy/

administrations to identify practices for improving the standards of protection of whistleblowers and the quality of reporting. Through a series of joint dialogues with ANAC, input from CSOs was integrated into the legislative transposition process of the Directive, influencing the inclusion of a public list of CSOs supporting whistleblowers on the ANAC website. In this way, potential whistleblowers who access the ANAC website to learn about the reporting procedures and related safeguards also become immediately aware of the support services dedicated to them. This has proven to have ripple effects, as other Italian public administrations have in turn adopted the good practice of increasing the visibility of civil society services by providing a direct link to their website.

- **Strengthening the competencies of public officials through a Community of Practice (CoP)**: Under leadership of the National School of Administration (SNA), the Community of Practice of institutional actors formally tasked with corruption prevention in Italian public administrations (RPCTs) was created: a collaborative space where RPCTs can exchange knowledge, share best practices, and enhance their capabilities to prevent corruption within their respective organizations. In order to strengthen public officials' capacities to handle whistleblowing reports and raise their broader awareness of whistleblowing, the CoP held 14 sessions on whistleblowing-related topics and exceeded participation targets. A comprehensive handbook was published to guide practitioners[34], and three best practices concerning whistleblowing have been developed[35]. Training and guidance materials are vital for promoting information on reporting systems internally and externally of public administrations.

To increase ownership over whistleblowing mechanisms, all obliged entities can promote training for their managers and employees. In the experience of CSOs, **training aimed at actors from all sectors should** move away from a law-centred approach and instead **adopt an ethical dilemma approach**. Through this methodology, which is experiential rather than theoretical, participants reflect on prototypical cases of misconduct, working both individually and in groups to identify possible solutions, including whistleblowing reports, helping them to simulate a report. Training modules can be organised in joint forms by institutions and other stakeholders, as in the example of 'Open the Whistle' project.

Further initiatives consistent with the OG principles of transparency and collaboration can be to promote **joint communication campaigns** between diverse stakeholders, following 'Open the Whistle' example, or to leverage national broadcasting media for communication projects with social value. Popular platforms, such as those related to sports or cultural events, can provide opportunities for communication directed at a very wide audience.

1.3 TRANSPARENCY OF INFORMATION SYSTEMS AND CHANNELS: FORMAL REQUIREMENTS

In relation to formal requirements, it should be noted that it is not enough to simply provide information and data on all the aspects previously described; rather, this information must meet a series of principles and formal requirements. That is to say, it should be provided in a **clear, correct, complete, and accessible manner**.

[34] In this regard see: https://sna.gov.it/wp-content/uploads/2024/09/WHISTLEBLOWING-cultura-integrita.pdf

[35] The first one emphasizes the need to view whistleblowers as a human anticorruption measure; the second best practice focuses on developing policies that treat whistleblowing as a duty rather than a risky activity, in order to eliminate social stigma and normalize the act of reporting wrongdoing; the third one emphasizes the role of Civil Society Organizations (CSOs), by providing a direct link to their website on the whistleblowing platform of PAs. https://sna.gov.it/home/attivita/comunita-di-pratica/comunita-di-pratica-per-rpct/buone-pratiche/whistleblowing-buone-pratiche/

For example, Spanish Law 2/2023 explicitly establishes that adequate information must be provided in a clear and easily accessible way and that:

> "If there is a website, such information must appear on the homepage, in a separate and easily identifiable section."

Moreover, access must be **universal**, meaning that all potential recipients must have equal opportunities to access the information. This requires adopting inclusive methods for all individuals. According to the **World Health Organisation (WHO)**, more than one billion people worldwide have some form of disability, and of these, nearly 200 million experience significant difficulties in their daily functioning[36]. The most common types of disabilities are usually: **visual, auditory, motor and cognitive**.

In this regard, for example, in Spain, both Royal Decree 1112/2018, of September 7, on the accessibility of websites and mobile applications of the public sector, as well as the Web Content Accessibility Guidelines (WCAG) developed by the World Wide Web Consortium (W3C), must be taken into account. Similarly, in Italy[37], Legislative Decree no. 76/2020, amending Law 4/2004 with the introduction of paragraph 1 bis to art. 3, extended the application of the accessibility obligations to private entities, in addition to the public sector websites, which were already required to be accessible.

In line with these guidelines, it is important to avoid certain practices on websites, such as placing "clickable" elements very close to each other, and using very small icons or text links with excessively small font sizes. It is also advisable to be aware of the correct contrasts between background and text color combinations. In this sense, the WCAG defines in Criterion 1.4.3, defines the parameters that must be followed when establishing color contrast[38].

Finally, it is recommended that, to facilitate **understanding** and **accessibility**, a section of frequently asked questions (FAQs) or explanatory videos on basic functioning of the whistleblowing channel be included. Additionally, when multimedia or audiovisual files are made available to users, they should include: subtitles, audio transcriptions, and video descriptions be incorporated to ensure access for individuals with hearing disabilities.

1.4 TRANSPARENCY OF INFORMATION SYSTEMS AND CHANNELS: ANNUAL REPORTS AND STATISTICS

The regular publication of system performance data in annual reports serves as an exercise of **good governance** and **accountability** and is also a way to build trust.

---

[36] Retrieved from: https://www.paho.org/es/noticias/5-12-2011-mil-millones-personas-viven-con-discapacidades#:~:text=M%C3%A1s%20de%20mil%20millones%20de,pues%20su%20prevalencia%20est%C3%A1%20aumentando

[37] In this regard see: https://www.agid.gov.it/it/ambiti-intervento/accessibilita-usabilita

[38] For example, for level AA, a contrast ratio of 4.5:1 between the background and the text is required.

As a good practice, it is recommended to provide statistical information **to the public and stakeholders**, at least annually, on the following areas:

A. number and typology of communications received;
B. number of communications accepted for processing;
C. number of communications dismissed after running the admissibility test;
D. number of communications investigated that ends in a resolution;
E. number of investigated communications that have led to the adoption of measures aimed at reducing or avoiding the risk factors detected;
F. number of communications investigated that were ultimately filed;
G. number of sanctions imposed or disciplinary proceedings initiated;
H. number of times the entity referred cases to the Public Prosecutor's Office, European Public Prosecutor's Office, Independent Authorities, or courts;
I. number of training sessions or workshops conducted for employees and managers on the reporting channel;
J. number of confidential reports and number of anonymous reports;
K. number and typology of inquiries made;
L. number of instances where the entity engaged an external company to hire investigative services or forensic compliance experts;
M. number and typology of support measures[39] or other measures voluntarily provided;
N. in the case of an organisation with international presence: number of communications received by geographic area;
O. number and typology of improvements made to the information system and channel;
P. general results regarding the level of satisfaction, awareness, and understanding of the system among its users.

It should be noted that these reports or annual accounts **must not include any personal data**, especially data that would allow for the identification or re-identification of whistleblowers, affected individuals, witnesses, or other third parties involved in any processes, even if such data has already been published as a result of a final judgement.

1.5 INTERNAL AND EXTERNAL AWARENESS COMMUNICATION ACTIVITIES OF WHISTLEBLOWING SYSTEM

Whistleblowing systems require well-designed communication strategies to ensure their accessibility and build trust among whistleblowers. However, several challenges persist, such as a lack of knowledge about reporting channels, the negative perception of whistleblowers in some cultures, fear of retaliation, and the absence of effective awareness campaigns.

[39] Described in Article 37 of Spanish Law 2/23, Art. Of Bulgarian Law, Art.18 of Italian Legislative Decree.

1.5.1 Internal Communication: Challenges and Best Practices

Lack of clarity and insufficient training

Interviews revealed that many employees are unaware of how to report wrongdoing, and internal reporting channels remain undocumented. To address this issue, it is advisable to implement periodic training sessions, integrate whistleblowing awareness into employee onboarding programs, and reinforce internal campaigns highlighting the importance of reporting. As a **good practice**, some companies have implemented QR codes with clear instructions to facilitate access to the reporting channel.

Distrust and negative perception

Whistleblowing is still perceived as an act of betrayal in some contexts. Interviews indicated that fear is the primary barrier, making a change in narrative critical. To overcome this, communication strategies must emphasize whistleblowing as a right and ethical responsibility, supported by testimonies from employees or leaders who emphasize its importance.

Integration with ethics and compliance policies

Interviews also indicated that many companies lack real commitment to managing reports. To strengthen these mechanisms, whistleblowing systems must be integrated into internal audits and risk control systems, ensuring their integration into corporate governance.

1.5.2 External Communication and Stakeholder Engagement

Lack of transparency and poor public communication

Many organisations fail to communicate effectively about their whistleblowing systems. A measure to change the narrative could be publishing statistics and success stories to build trust. The proliferation of poorly managed reporting channels has created confusion rather than fostering their use. To improve this situation, it is suggested:

A. to inform adequately, on the one hand, about all the elements highlighted in Section 2 of this Chapter in a clear, correct, complete, and accessible manner, and on the other, to publish annual reports and;
B. develop strategic awareness campaigns and sensitization key actions in collaboration with civil society.

Role of civil society and the media

According to the interviewees, civil society can play a pivotal role to enhance transparency, since at times the stigma surrounding whistleblowing continues to affect whistleblowers and limit their participation. To overcome this issue, establishing dialogue channels with the media and NGOs is necessary to strengthen accountability and broaden the reach of whistleblowing mechanisms.

FINAL RECOMMENDATIONS

1. GREATER CLARITY

Greater clarity in internal reporting channels and processes is crucial

2. PERCEPTION CHANGE

Changing the perception of whistleblowing as an ethical tool is key.

3. ENSURING TRANSPARENCY

Ensuring complete and meaningful transparency[40] is critical to ensuring greater trust[41].

4. INCLUSIVE STRATEGIES

Inclusive strategies with a gender perspective and protection for whistleblowers are necessary.

5. TRAINING

Train workers and citizens and also those responsible for managing the reporting systems.

Strengthening **transparency and communication** will help **establish an effective, accessible, and trustworthy whistleblowing culture**, promoting **integrity within organisations**.

[40] It is very important to explain on the websites the steps to explain to whistleblowers what they have to do and what the procedures and their rights and obligations are.

[41] According to one of our interviewees, it would be also important for Administrations to also include tools, resources and contact data on civil society organisations that support whistleblowers.

Proper investigation and management in internal whistleblower systems

Chapter 2

Open the whistle

PROPER INVESTIGATION AND MANAGEMENT IN INTERNAL WHISTLEBLOWER SYSTEMS

Chapter 2

2.1 KEYS TO PROPER INVESTIGATION

Within the mission of preserving the public interest, the legal framework defined by the Directive depends upon a condition crucial to its effectiveness: *trust in the system*. When an internal report falls within the scope of the Directive, an internal investigation may be initiated which shall comply with all the legal guarantees and be diligently followed up. Internal and external reporting channels must provide adequate safeguards against potential *reprisals*, which constitutes a keystone for encouraging reporting persons to come forward and break the silence.

Article 7(1) and 7(2) of Directive establish the principle that reporting persons are free to choose whether to first report internally or directly via external channels. External reporting is particularly envisaged in situations where the breach cannot be effectively addressed internally, or when the reporting person believes there is no risk of retaliation (see art. 7 (2)). Several Member States (which are not identified in the report) incorrectly impose an obligation to report internally first or permit direct external reporting only under specific circumstances. Additionally, some Member States have failed to explicitly provide protection for individuals reporting to EU institutions. In this context, internal reporting is the most appropriate means of collecting information for an early resolution of threats to the public interest. For this reason, **internal reporting channels are given preference**, though internal reporting is not a mandatory prerequisite for submitting reports externally.

The second meeting of the European Commission's expert group on the Directive[42] notes that when whistleblowers report directly via external channels, organisations are unable to promptly remedy the situation or irregularity. Consequently, organisations must set up clear, easily accessible, and effective internal channels, and foster a **corporate culture** that actively encourages internal reporting of breaches**.** Internal investigations arising from communications or information received via internal channels, whether within a public or private organisation, are conducted **in the public interest**.

[42] The European Commission's expert group is an advisory group made up of experts representing the Member States of the European Union with responsibilities for the transposition of the Directive 2019/1937/EU. Its fundamental mission is to draw up recommendations to the Member States for the transposition of the Directive 2019/1937/EU.

Internal reporting procedures and their follow-up must meet certain fundamental requirements to achieve their intended purpose and comply with the provision of the Directive and national legislation. These requirements are essentially as follows:

A. internal channels must enable individuals within the personal scope of the Directive to report breaches covered by its material scope and national transposition laws;
B. channels must be designed, established, and managed securely to ensure confidentiality of the reporting person's identity and of any third party mentioned in the report, while also protecting personal data from unauthorised access;
C. an acknowledgement of receipt must be issued to the complainant within seven days of receipt of the report;
D. communication with the complainant may be maintained during the processing of the report, and additional information may be requested if necessary;
E. channels must enable diligent follow-up and effective processing of the communications submitted, including anonymous ones, when applicable;
F. feedback regarding the follow-up of the report must be provided within a reasonable timeframe, which shall not exceed three months from the acknowledgement of receipt to the complainant or, if no acknowledgement is issued, within seven days of the report being submitted;
G. clear and accessible information must be provided concerning the external channels managed by competent national authorities and, where applicable, of the EU institutions or bodies.

GENDER BOX

Implementing gender-sensitive channels and targeted policies would enhance the effectiveness of support processes, particularly for women and other vulnerable groups.

Specific **recommendations to ensure gender sensitive reporting mechanisms can** include:

A. **inclusive Design and Representation**: ensure the participation of women and diverse gender identities in the design of reporting mechanisms and policies;
B. **gender-Sensitive Protocols and Coordination**: establish gender-based protocols for each internal reporting channel. Coordinate efforts between code of conduct, anti-corruption and gender-based violence reporting mechanisms;
C. **gender-Sensitive Reporting and Investigation Systems with Comprehensive Support Services**: clear guidelines for gender-based cases, with trained personnel to handle reports sensitively. Inform whistleblowers about external support services, such as legal aid, psychological support, and survivor advocacy organisations;
D. **gender-Sensitive FAQ and Support Channels**: develop a dedicated channel for inquiries related to gender-based misconduct. Provide a Frequently Asked Questions (FAQ) section or clear reporting guidelines for gender-related issues;
E. **awareness and Training**: conduct gender-based awareness and sensitization training within organisations hosting reporting channels. Address gender stereotypes and biases to ensure an inclusive and effective whistleblowing system.

2.2 CHALLENGES OF INTERNAL INVESTIGATION S

Internal investigations **aim to verify the veracity or plausibility of the reported** facts and to identify the individuals responsible for the violation or irregularity in question. It is particularly important—both for the validity of the internal investigations themselves and for ensuring compliance with the Directive and national laws—that any methods used to gather evidence respect fundamental rights in all cases. (For more details regarding the protection of fundamental rights, see Chapter 1).

Ch. 1 ›

What are the challenges that may arise during internal investigation?

A. maintaining the **confidentiality** of personal data can be complex and requires implementing specific technical, **organisational and security measures** (such as restricted and hierarchical access, double authentication, internal anonymisation, etc.) explicitly designed for this purpose. During **internal investigations**, the whistleblower's identity might be uncovered or deduced inadvertently, as certain characteristics (e.g., gender, job position, associated project, etc.) may indirectly r**eveal their identity.** Additionally, requesting information from other departments or conducting personal interviews may inevitably broaden the **circle of individuals** aware of the investigation and potentially the identity of the whistleblower;

B. ensuring **confidentiality of the identity of whistleblowers,** especially when internal reporting channels are outsourced to a third party (subcontractor). Such outsourcing must comply with **Recital 54 of the EU Directive**, which specifies that **third parties** may include external reporting platform providers, external counsel, auditors, trade union representatives, or employee representatives. Outsourcing inherently increases the number of individuals with access to sensitive information. Therefore, **explicit guarantees of independence** and confidentiality must be clearly outlined in the contractual agreement between the organisation and the external third party. According to Article 8(5) of the Directive, in the event of a breach, both the third party and the legal entity share responsibility. **Experts consider that joint liability** is the most effective way to protect whistleblowers' rights, allowing the reporting person to initiate legal actions against the entity, the external third party, or both;

C. experts also consider that **handling the identity of a whistleblower** constitutes "processing of personal data", within the meaning of the General Data Protection Regulation (GDPR). Consequently, **penalties** for disclosing the whistleblower's identity should be more severe than **sanctions** generally provided by national laws for other breaches of p**ersonal data confidentiality**. This heightened severity is necessary because disclosing the whistleblower's **identity can expose** them to retaliation and weaken trust in the whistleblowing system itself;

D. penalties for breaches of confidentiality have been incorrectly transposed in certain cases—for instance, due to a **lack of appropriate cross-references** to applicable legislation. This situation is particularly concerning, first due to the lack of harmonisation of **European protection standards,** and second, because it undermines one of the cornerstones of European whistleblower regulation;

E. during internal investigations, private interests of organisations also

come into play. Consequently, in certain contexts, internal investigations into breaches and irregularities are seen as mechanisms of **public-private collaboration**. However, interviews conducted in Italy have highlighted a specific challenge: conflicts of interest may arise when the content of the whistleblower's report conflicts with the interests of the organisation.

OPEN GOVERNMENT BOX

Effective investigation and management in internal reporting systems require **transparency and well-defined guidelines** to ensure consistency and fairness across different sectors, including the public sector, private sector, and non-profit organisations. Such guidelines can be developed through a co-design approach, involving public authorities responsible for whistleblowing and interested stakeholders. This collaborative process can take place through **dialogues or public consultations**, as demonstrated by the Italian National Anticorruption Authority (ANAC).

In 2024, ANAC launched an online public consultation[43] to collect feedback on its draft guidelines for whistleblowing. The objective was to promote a uniform and effective application of whistleblowing legislation while reducing interpretative uncertainties for entities managing internal reports in both public and private organisations. The ANAC model provides a useful framework that other countries could replicate to enhance stakeholder engagement in the development of whistleblowing guidelines:

A. an open online consultation period lasting at least one month to allow ample time for feedback;
B. a user-friendly platform for submitting contributions (e.g., online questionnaires);
C. widespread dissemination of the initiative across multiple relevant forums to ensure visibility and encourage participation;
D. targeted invitations to key stakeholders actively engaged in whistleblowing processes.

Practitioners recommend designating a dedicated **Point of Contact within the public authority responsible for whistleblowing**. This individual would act as a resource for managers of internal reporting channels, providing guidance and resolving challenges in report management and investigation. Additionally, concerns related to the proper investigation of reports could be addressed through peer meetings between internal reporting channel managers and the public authority. To foster collaboration and continuous improvement, the creation of a **working group or Community of Practice** on whistleblowing could be incorporated into Open Government Partnership, whether as part of the regular National Action Plans or as an Open Gov Challenge commitment.

A further key aspect in facilitating a proper investigation is ensuring the high quality of whistleblowing reports. One effective way to design a strong internal reporting system—one that is as accurate as possible and aligned with the actual risks faced by the organisation (whether public or private)—is to conduct a

[43] In this regard see: https://www.anticorruzione.it/en/-/news.07.11.24.lg.whistleblowing

participatory risk assessment of potential misconduct that could emerge through whistleblowing.

Ideally, this process should involve multiple departments, areas, and sectors within the organisation. However, particularly in the case of public institutions, it can also be carried out using Open Government principles by engaging civil society in shaping the process. External input can provide a broader perspective and deeper understanding of environmental and contextual factors, helping the organisation identify risks that may otherwise be overlooked or underestimated. The outcome of this process is a reporting system that includes well-defined case scenarios, tailored to a deeper understanding of the organisation's risks. This not only supports whistleblowers in drafting clearer and more precise reports but also ensures a more effective and thorough investigation.

2.3 GENERAL FRAMEWORK OF THE INVESTIGATION PROCEDURES

Article 9(1) of the Directive establishes that the internal reporting procedure must include **diligent follow-up** by the person or department designated for this purpose. (See Chapter 1 for transparency in whistleblowing procedure).

In this regard, Article 5.12 of the Directive defines "follow-up" as:

> "any action taken by the recipient of a report or any competent authority in order to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure"

Therefore, the Directive includes two actions in the concept of **diligent follow-up of the report:** the assessment of the accuracy of the issues reported and the resolution of the reported infringement.

According to the **Report on the Implementation of the Directive**, several components of this provision (Article 9)—such as the obligation to diligently follow up on reports, the deadlines for issuing an acknowledgment of receipt, or arranging physical meetings – have not been correctly transposed in most Member States. National transposition legislation generally establishes a **certain minimum content and/or principles** for internal reporting procedures, though it does not typically regulate them in detail. Thus, obliged entities retain some discretion to self-regulate and organize internal investigations, provided they respect the principles and minimum requirements defined by national law. This allows procedures to be better adapted to the characteristics of each organisation.

In **Spain**, **Article 9(2)** of **Law 2/2023** stipulates that the internal reporting procedure must comply with a set of minimum principles and

requirements, including clearly identifying internal and external reporting channels, issuing an acknowledgment of receipt to the whistleblower within seven days, and establishing a maximum deadline of three months for responding to investigations, extendable in complex cases. Furthermore, continuous communication with the whistleblower must be enabled, guaranteeing their right to be informed about the progress of their report. Confidentiality, presumption of innocence, personal data protection, and respect for the honor of those involved must also be ensured. If reported facts potentially constitute a criminal offense, the information must be forwarded to the Public Prosecutor's Office or, if the EU's financial interests are implicated, to the European Public Prosecutor's Office.

A similar requirement exists in **Italy**, where **Article 4 of Legislative Decree 24/2023** states that both public and private sector entities must establish channels ensuring confidentiality of the reporting person's identity, the persons involved or mentioned in the report, as well as the content of the report and accompanying documentation, including through encryption tools.

The procedures and protocols approved by the obliged should clearly outline the general principles governing internal reporting channels and the protection of whistleblowers within the organisation. These procedures must be formally approved by the entity's administrative or governing body. Additionally, they must be published and communicated effectively to all potential users of the channel. Proper dissemination is essential, as it helps prevent misuse of the channel and reduces submissions that cannot be appropriately processed.

2.3.1 Investigation procedure : guidelines, principles and guarantees

To **ensure legal certainty** in internal investigations and to **protect the investigators themselves**, it is **highly advisable that** internal report management procedures be detailed comprehensively. Beyond the minimum content and principles outlined by national transposition laws, internal procedures **should explicitly describe** each phase of the reporting management process, **specifying actions** to be performed in each phase. These procedures should also regulate verification methods and outline appropriate measures for preserving and safeguarding documentation and evidence gathered during investigations.

The phases of the internal reporting procedure that could be included in the procedure are the following:

A. report reception phase;
B. report admission or dismissal phase;
C. investigation phase;
D. action completion or termination phase.

2.4 REPORTING PERSONS' RIGHTS

The person reporting has the **fundamental right** to file a confidential report and not disclose their identity, where permitted by national legislation.

Anonymous reporting

The Directive and any transposing legislation establish an obligation to maintain the confidentiality of the whistleblower's identity and of the content of the report. Regarding anonymous reports, the Directive allows for different national approaches, as not all Member States accept anonymous reporting. However, where it is permitted, **communication with anonymous reporting persons must be guaranteed**.

In the **Report on the Implementation of the Directive** issued by the Commission, it is emphasized that if Member States require entities to accept anonymous reports, **such reports must be handled with the same procedural rights as non-anonymous reports**. This includes both the rights of the reporting person and the obligations of entities and authorities to conduct diligent follow-up.

Since an internal investigation may lead to **disciplinary, sanctioning, or criminal proceedings**, evidence must be obtained in compliance with applicable laws, procedural rules, and the rights of all parties involved. These include **fundamental rights, labor rights, rights established in the Directive and national law, as well as the internal procedures and protocols approved by the organisation**.

A widely recommended **best practice** is to protect complainants' rights through **joint liability**, enabling them to take legal action **against the entity, against the external third party managing the reporting system, or against both:**

A. to file a report verbally or in writing;
B. to choose whether to report through the internal channel, unless they have valid reasons to report externally;
C. to receive confidential, and free legal advice at the time of reporting.

This advice should clarify:

A. whether the reported information falls within the scope of whistleblower protection rules;
B. the most appropriate reporting channel to use;
C. alternative procedures in case the information does not fall within applicable whistleblowing regulations;
D. available protection and support measures;
E. to receive an acknowledgement of receipt for their report;
F. to access protection and support measures, including financial

assistance and psychological support in certain cases, provided the whistleblower meets the conditions for protection. This includes cases where they reported anonymously, were later identified, and suffered retaliation;

G. to be informed about the status of their report and to receive updates on the outcome of the investigation;

H. to maintain confidentiality and protect their identity throughout the process;

I. to have their personal data processed in accordance with the rights conferred by European legislation and national law on this matter.

Member States, in their transposition laws, may **introduce provisions** more favourable to whistleblowers' rights than those established in the Directive. It is important to note that, in order to qualify for protection, whistleblowers must not only report through the channels provided in the Directive but also have **reasonable grounds to believe that, based on the information available to them at the time of reporting, the facts they disclose are true**. Protection **does not extend** to **abusive, malicious, or false reports**.

The **accused person** should have the following fundamental rights:

A. to have their identity preserved;

B. to be informed and to be heard, in a manner and time frame deemed appropriate to ensure the effectiveness of the investigation;

C. to access the content of the file of the investigative actions and to make allegations;

D. to the presumption of innocence and the right to honour;

E. to receive information on the measures taken that affect them as a result of the investigation;

F. to have their personal data processed in accordance with the rights conferred by European legislation and national law on this matter.

According to **Recital 76 of the Directive,** Member States must ensure that competent authorities have **adequate procedures in place** for processing reports and protecting the personal data of individuals mentioned in the report. **These procedures must guarantee** the protection of the identity of each reporting person and each affected person, but also of third parties mentioned in the report, such as witnesses or co-workers, in all phases of the procedure.

2.4.1 Rights linked to the processing of personal data

Regarding the rights linked to the **processing of personal data**, when the data are obtained from the interested party, the information indicated in art. 13 of Regulation (EU) 2016/679 must be provided.

The reporting persons, the accused persons as well as the **third parties** mentioned in the reports and in the investigations may exercise the rights recognized by articles 15 to 22 of Regulation (EU) 2016/679 (right of access of the interested party, right of rectification, right of deletion, right to limitation of processing, obligation of notification regarding the rectification or

deletion of personal data or limitation of processing, right to data portability, right of opposition, right not to be subject to automated individual decisions, including profiling).

However, in some cases, national transposition laws **have restricted the exercise of certain rights**. For instance, the right to object to the processing of personal data by competent authorities has been limited in some jurisdictions.

2.5 INTERNAL REPORTING STRUCTURE AND RESPONSIBILITIES

The decision **to designate a responsible person** for the internal reporting channel - and, where applicable, additional personnel to manage report follow-up procedures (as established in some countries, such as **Spain**) - should be made transparently. This means that potential users of the channel **must be informed** of the identity of these individuals. The persons responsible for managing the internal channel **must possess the necessary technical expertise**, as well as the skills and **competencies required** to conduct internal investigations effectively. However, **this transparency requirement also presents challenges,** particularly in establishing effective communication platforms for individuals outside the organisation (e.g., contractors, former interns).

From a practical standpoint, **especially in large organisations**, it may be practically impossible for a single person or department **to handle all internal reports** submitted through the channel. Additionally, Article 16 of the Directive mandates that Member States **ensure the identity** of the reporting person is not disclosed without their explicit consent, except to an authorised staff member responsible for handling or following up on reports, as defined in Article 5(12) of the Directive. This provision implies that **a team of individuals**—with the necessary technical training and bound by strict confidentiality obligations—**may be involved in monitoring reports,** analysing cases from different perspectives, or performing different investigative functions.

Therefore, **it is recommended to:**

A. **make an explicitly reference to** the existence of the reporting channel, in compliance with the transparency obligations set out in the EU Directive in contractual clauses or supplementary documents;
B. **designate in advance** an alternate person who can **temporarily or permanently** replace the responsible individual managing the internal reporting channel in cases of vacancy, absence, or illness. This **replacement mechanism** is also essential in situations where the **primary channel manager** must recuse themselves due to conflict of interest or other legally established grounds;
C. **fully inform any individuals affected by a report of the investigative procedure** and of the identity of the individuals responsible for conducting the internal investigation.

Furthermore, accused individuals must be able to trust that the designated people will act **objectively and impartially**.

By ensuring that reports are processed and investigated by neutral and competent professionals, organisations will increase trust and effectiveness in the internal reporting system. This, in turn, will reinforce confidence among all potential users that the reporting channel operates properly and reliably, and that reports are taken seriously and handled diligently. Having such a provision is crucial to ensuring objectivity and impartiality in internal investigations.

2.5.1 Organisational structure of internal reporting systems

The administrative or governing body of an entity may designate the **individual(s) responsible for managing the internal reporting channel** and handling the reception and follow-up of reports, as is the case under **Spanish** and **Italian** legislation. For the system to be effective and credible, all communications must be managed efficiently and diligently within the organisation itself. This responsibility could fall on the person in charge of the internal reporting channel. Therefore, it is essential that these individuals, due to their position within the organisation, are able to perform their duties **independently and autonomously**, without being subject to any external influence, and with access to all the personal and material resources necessary to fulfill their role. As previously mentioned, the specific circumstances of each organisation may justify assigning this responsibility to a team rather than a single individual. In addition to benefiting from collective decision-making, such a team could also bring a multidisciplinary perspective to investigations.

The selection of appropriate professionals may vary depending on the type and structure of the entity. However, those responsible for managing the internal reporting channel must be committed to regulatory compliance, integrity, and the ethical principles and values of the organisation. Since these individuals must perform their **functions independently and autonomously, and in any case avoiding conflicts of interest**. Ultimately, the credibility of the internal reporting system **depends on the trust employees place in those responsible for handling reports**. If employees perceive that reports are managed objectively and effectively, they will be more likely to use the internal channel.

In smaller entities, this could be a dual function carried out by a company executive who is well placed to **communicate directly** with the entity's management, for example, a compliance or human resources officer, an institutional integrity officer, a legal or privacy officer, a financial officer, an audit officer or a member of the board of directors.

In general, the person responsible for the internal channel may incur in responsibilities arising from the management and correct functioning of the internal system. Such responsibilities may relate to the diligent treatment and follow-up of reports, relating to the **guarantees of protection**

of the informant within the organisation itself, as well as relating to their behaviour when they have to interact with the competent authorities. In addition, in certain cases, the person responsible may incur **criminal liability** if the conduct is typified in the applicable criminal legislation (for example, disclosure of secrets, crimes committed by public officials).

In any case, it will be necessary to take into account the obligations established by the national transposition legislation of the Member States for the purposes of determining the specific responsibilities of the persons responsible and managers of the internal channel in each case.

2.5.2 Conflicts of Interest in Internal Reporting Systems

Conflicts of interest arise in situations where the impartiality and objectivity of individuals responsible for making professional judgments are compromised by a personal or external interest. Like any risk, conflicts of interest can and should be managed proactively. To ensure fairness and credibility, internal report management procedures must explicitly include measures for identifying, managing and addressing conflicts of interest that may affect those responsible for handling and investigating reports.

This guarantees that individuals conducting internal investigations remain impartial and objective.

A **reactive approach to conflicts of interest -** waiting until a conflict arises before determining how to handle it **- is not advisable**. Instead, organisations **should anticipate and establish** clear procedures to address such situations. Failure to do so **may undermine trust** in the internal reporting channel, as concerns about bias or lack of impartiality could arise, leading to a loss of credibility in the management of reports.

A recognized **best practice** is to require investigators to complete a "Declaration of No Conflict of Interest" before initiating an internal report procedure. This helps ensure that the assigned personnel do not have personal or professional ties that could affect their neutrality.

Investigations have a **time limit**. They must last for the necessary time, which may not exceed the three-month period, except in cases of particular complexity, in which the proceedings may be extended for an additional three months. The extension of three additional months should be adopted prior to the conclusion of this first period, setting out the causes that have prevented the completion of the investigations and the pending proceedings, justifying the reason for the adoption of this extension.

2.5.3 Data protection considerations

Article 17 of the Directive establishes that any **processing of personal data** carried out in the implementation of it, must comply with the Regulation (EU) 2016/679 and the Directive (EU) 2016/680. Additionally, **any exchange or transmission of information** by EU institutions, bodies, offices, or agencies

must be carried out in accordance with Regulation (EU) 2018/1725, which governs data protection within EU institutions.

This article also incorporates the principle of data minimization, which aims to prevent the collection of unnecessary data for the investigation of a report. If irrelevant data is accidentally collected, it must be deleted immediately.

However, it is also essential to consider national legislation regarding specific aspects such as access to personal data contained in the internal channel, report register, and investigation files, as well as data retention periods established by national law.

According to Recital 83 of the Directive, special attention should be given to the fundamental principles of personal data processing as established in art. 5 of Regulation (EU) 2016/679, Article 4 of Directive (EU) 2016/680 and Article 4 of Regulation (EU) 2018/1725, and the principle of data protection by design and by default set out in Article 25 of Regulation (EU) 2016/679, Article 20 of Directive (EU) 2016/680 and Articles 27 and 85 of Regulation (EU) 2018/1725.

It is important to recall the content of Article 5 of Regulation (EU) 2016/679[44] which establishes that the **guiding principles to guarantee** the legitimacy of the processing of personal data are the principle of proactive responsibility, the principle of legality, loyalty and transparency, the principle of purpose limitation, the principle of data minimization, the principle of accuracy, the principle of limitation of the conservation period and the principle of integrity and confidentiality. (To read exhaustive detail see **Chapter 3**).

Ch. 3 >

[44] 1. Article 5. Personal data shall be:
a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

2.6 INVESTIGATION PROCESS WITHIN THE INTERNAL REPORTING SYSTEM

It is advisable to establish a system for identifying reports, along with a record of the information received and the internal investigations conducted. Special attention must be paid to the limitation of personal data retention periods, see Chapter 3 to explore the topic in depth. During the report reception phase, the whistleblower must receive an **acknowledgment of receipt within seven days**. This confirmation is essential, as it serves as proof that the whistleblower has submitted a report through the **internal reporting channel.** It may also be required when requesting protection measures and/or support from the competent authority.

Ch. 3

Once a report is received, the next phase of an internal investigation protocol could be determining the **admissibility of the report**. The person responsible for the internal channel must assess the report and decide—with justification—on one of the following options:

A. inadmissibility of the report;
B. admission of the report for processing;
C. referral of the report to the Public Prosecutor's Office, the European Public Prosecutor's Office, or any other competent authority, entity or body.

Examples of inadmissibility criteria

A report may be deemed inadmissible under the following circumstances:

A. unintelligible, implausible allegations, including prima facie false reports with no objective basis;
B. reports lacking a minimum description of the facts, such as the time, location, or nature of the alleged infringement or irregularity;
C. reports based purely on hearsay, speculation, rumors, or assumptions;
D. reports concerning identical facts already investigated and resolved by the organisation, unless new evidence or significant information is provided.

Regarding the first cause of inadmissibility— prima facie false reports— Recital 101 foresees the retention of protection when facts reported where inaccurate or misleading under the rules of general national law. However, Article 23 of the Directive requires Member States to impose sanctions for knowingly false or malicious reports, in order to prevent new false or malicious reports and preserve the credibility of the system. These sanctions must be proportionate, ensuring they do not create a deterrent effect on legitimate whistleblowers. When dealing with false reports, entities must comply with national transposition laws governing this matter.

According to the Report on implementation of the Directive issued by the EU Commission, regarding **this sanctioning regime** some compliance issues was detected regarding national transposing legislation, for instance the following:

A) lack of legal certainty on what constitutes sanctionable conduct;
B) ineffectively low fines, reducing deterrence;
C) penalization of retaliation only against reporting persons, rather than extending protection to other categories of individuals, such as facilitators (Article 4 of the Directive).

Under **Italian law**, a report may be considered **inadmissible** in the following cases:

A. when there is a lack of data which constitute essential elements of the reports (e.g. the facts reported and the Administration or Entity in which they occurred; the Administration or Entity in whose working context the whistleblower operates and the professional profile held by the latter; a brief description of the ways in which the whistleblower became aware of the facts reported etc.);
B. when the reported violations do not fall within the material scope defined by the Italian law;
C. when the reporting person is not among those legally authorised to report;
D. when the reported facts do not relate to the work environment.

2.6.1 What happens when the report is admitted for processing?

The content of the report is subjected to the **verification of the plausibility: everything that** does not offer any note or element of falsehood can be defined as plausible. A report is considered **plausible** when there are **sufficient indications to justify further inquiries**. Conducting a thorough plausibility assessment is crucial to avoiding arbitrary or unnecessary investigations. The plausibility of a report must be continuously reassessed throughout the investigation phase, ensuring that evidence collected aligns with the reported facts. After, the person allegedly responsible is identified and evidence collected.

This is also the time to **adopt any interim measures in order to ensure the effectiveness** of the investigation and avoid damage that may be irreparable at a later stage. These interim measures must be planned in the internal procedure and in a motivated manner and after carrying out a prior analysis of the necessity and proportionality of them.

2.7 INVESTIGATION POWERS

The primary objective of an internal investigation is to gather and preserve evidence necessary to establish the facts and determine possible liabilities. **Internal investigations** do not have the same scope or l**egal nature** as

judicial investigations, as they are of an administrative nature. Any collection of evidence **must strictly avoid** the use of illegal, unfair, or unethical methods that infringe upon fundamental **rights and freedoms**, both individual and collective[45]. An investigation that fails to respect these evidentiary limits may result **in serious consequences**, including invalidation of the evidence obtained and **potential criminal liability** for those conducting the investigation. Fundamentally, internal investigations rely on **various means of verification**, the most common being:

A. documentation and/or information that incorporates data and evidence, and;
B. personal interviews.

To verify the accuracy of reported facts, investigators typically request **documents and reports** containing necessary data as evidence.

This data sources can be categorized into:

A. **internal sources**: Various organisational units must collaborate with the investigation, as they may hold valuable records that clarify the circumstances of the case;
B. **open sources**: among the many that can be consulted, we suggest some:
   I. public procurement and procurement data can be obtained by consulting registers and platforms with public procurement data and on the open data portals of public sector entities;
   II. commercial data can be obtained in public commercial registers and in official bulletins;
   III. data from public sector administrations and entities such as general data, budgets or annual accounts, elected officials, managers and staff, organisational charts, and others can be found on the transparency and open data portals of these organisations;
   IV. data regarding grants and subsidies can be obtained from subsidy registers, open data portals of different entities and also in official bulletins;
   V. electoral roll data can also be obtained from open sources;
   VI. data from the Register of Interest Groups;
   VII. data from the agendas of high-ranking officials.

When using open sources, it is crucial to **assess the reliability of the information**. Open-source data must often be filtered, validated, and cross-checked to ensure accuracy. **A good practice to preserve confidentiality is not to request that documentation from the departments or units of the organisation itself if that information can be obtained by consulting open sources.**

[45] It is recommended to consult the judgment of the ECHR 2017/169399 of September 5, 2017, case Bărbulescu v. Rumania (Barculescu II) on the recognition of private life in the work context.

2.7.1 What are the recommendations regarding personal interview?

A. conduct interviews with at least two investigators present;
B. foresee the conditions of discretion for interviewing people and how the interview should be documented and recorded, as well as providing the necessary information regarding the processing of their personal data according to the provisions of RGPD (art. 15 and following);
C. the first person to be interviewed should be the reporting person (if they are not anonymous). Then the interview should continue with people who may have information or may have been witnesses to the reported facts or conduct and, lastly, the possible participants and/or those responsible for the facts;
D. foresee whether the interviewee can attend in the presence of an attorney or other individual (facilitator, union representative etc).

2.7.2 Closing an internal investigation

An **internal investigation must be closed** when it is found unfounded or unsubstantiated.

If the reported facts are confirmed, the possible ways of **finalising** the internal investigation are as follows:

A. **communication to the competent department** or unit so that it can adopt measures to resolve the reported infringement, such as, among others, disciplinary measures;
B. **transfer to an administrative competent authority** when the infringement is confirmed;
C. **transfer to the Public Prosecutor's Office** and/or other judicial authority, when the reported facts integrate a criminal offence. If the possible criminal action affects the financial interests of the European Union, the report will be transferred to the European Public Prosecutor's Office;
D. internal recommendations in the event of having detected bad practices and lack of professionalism.

2.7.3 From the internal investigation to the Public Prosecutor's Office

The obligation to **transfer information** from an internal investigation **to the Public Prosecutor's Office or judicial authorities** has been incorporated into Spain's transposition of the Directive. However, this provision has been **controversial**, particularly for **legal entities subject to corporate criminal liability**. In some cases, mandatory reporting could conflict with the right against self-incrimination for legal entities. This can add complexity to certain investigations and raises legal challenges. The report **management procedure** must provide for the possibility of issuing **recommendations** to determine the treatment that these situations deserve and to be inserted into processes of continuous improvement of the organisation. Otherwise, it

would lose its reason for being a system that is originally conceived as an opportunity to also strengthen the institutional integrity system and the ethical and compliance culture of the organisation.

The recommendations resulting from an internal investigation can serve various purposes, such as:

A. to develop training or awareness-raising programmes;
B. to improve internal processes or protocols;
C. to ensure proper implementation of corrective measures;
D. to report to the compliance oversight body regarding adherence to the code of ethics or conduct, etc.

Both **the person accused** by the report and **the reporting person** must be **informed of the investigation's outcome**. The Directive recognizes the right of the reporting person to receive updates on the status of their report and to be informed of the investigation's final results.

It is **advisable that the report or document that concludes** the actions include how the investigation was initiated, the object of the investigation, the i**nvestigative actions carried out,** who has intervened, the assessment of the accuracy of the facts, as well as the conclusions and proposals that **finalize the follow-up** of the report received in order, as the **Directive states**, to resolve the reported infringement. It must, in any case, be objective, impartial, clear and precise.

2.8 THE ROLE OF THE EXTERNAL REPORTING AUTHORITY

2.8.1 The Importance of Effective Whistleblower Reporting Channels

According **to Recital 63** of the Directive, **lack of confidence in the effectiveness of reporting channels** is one of the main factors discouraging potential whistleblowers. To address this issue, competent authorities are required t**o establish independent and autonomous** external reporting channels that ensure diligent **follow-up of reports** received and provide timely responses to whistleblowers. In cases where internal channels do not exist, have failed to function properly, or when **whistleblowers fear retaliation**, competent authorities may be better suited than the organisations themselves to handle and follow up on reports. **Article 11** of the Directive mandates that these external reporting channels must be both independent and autonomous in the receipt and processing of reports concerning legal infringements. Additionally, **Recital 65 emphasizes** that competent authorities must have the necessary capacities and powers to conduct proper follow-ups, assess the accuracy of reports, address infringements through investigations or prosecutions, and take corrective measures as required. If necessary, **authorities must** also be able to refer cases to **another competent body** to ensure appropriate follow-up.

2.8.2 Implementation Challenges and the Role of Competent Authorities

The implementation of the Directive **has faced challenges**, with some Member States failing to designate competent authorities with legal certainty. Additionally, about half of the Member States **have incorrectly transposed Article 11(6)**, which outlines obligations for authorities receiving reports but lacks the competence to address them. For example some states impose these obligations **only on specific authorities**, fail to ensure secure and timely transmission of reports, or omit the requirement to inform the reporting person.

When external reporting channels are centralized, Member States must ensure compliance with the Directive's independence and **autonomy requirements**. Articles 12 and 18 of the Directive establish strict criteria for external reporting channels, including guaranteeing the integrity and **confidentiality of information**, long-term storage, and **accessibility** for both written and oral reports, including anonymous submissions where permitted by national law. **Article 13** requires competent authorities to publish clear and accessible information on reporting procedures, appeals, **protection against retaliation**, and confidential advice for whistleblowers. Furthermore, **periodic reviews must be conducted** every three years to ensure reporting procedures remain effective. Competent authorities not only manage **external channels** but may **also impose sanctions** and play a vital role in promoting a culture that encourages whistleblowing, ensuring that those who report wrongdoing are not stigmatized or retaliated against.

2.8.3 Concurrent reporting to internal and external channels

Although the Directive does not require whistleblowers to report internally before using external channels, it does not explicitly address how to handle simultaneous internal and external reports. This issue was discussed in the **fourth meeting of the expert group**, where recommendations were made for Member States to include provisions in their transposition laws:

A. whistleblowers should wait for the three-month period to expire before reporting externally;
B. if they choose to report externally before the three-month period ends, they should withdraw their internal report.

Additionally, national laws could allow authorities to ask whistleblowers for consent to notify their employer about their external report. However, whistleblowers would never lose their protection for following these recommendations.

According to the EU Commission, in practice, the external report would result in the implicit withdrawal of the internal report. If the employer becomes aware of an external investigation, the internal channel would no longer be required to follow up on the report. However, the organisation

may still choose to continue its internal investigation. If both internal and external investigations proceed simultaneously, competent authorities remain obligated to investigate and address violations under the Directive.

In any case, the transposition laws should address how to deal with the concurrence of reports through the internal channel and the external channel when the whistleblower reports externally before the three-month period for the internal investigation has expired, following the recommendations made by the expert group.

FINAL RECOMMENDATIONS

1. PRESERVING CONFIDENTIALITY

Procedural, technical, organisational, and security measures must be implemented to preserve the confidentiality of personal data contained within internal reporting channels. Special emphasis must be placed on ensuring and safeguarding the confidentiality of the identity of both the whistleblower and the individuals affected by the report. Internal investigations must also be conducted in a manner that minimizes the risk of breaches of confidentiality throughout the entire process.

2. MONITORING PROCEDURES

The procedures for managing and monitoring internal reports must be detailed and addressed, in addition to the minimum content and principles provided for in the transposition laws, the different phases of the report monitoring procedure in the most complete way possible and specifying the actions to be carried out in each of them. They should also establish what the means of verification will be.

3. REPORT IDENTIFICATION

A report identification system must be in place, along with a record of received reports and conducted investigations. This ensures traceability of the internal channel's operations and enhances accountability.

4. DETERMINE ADMISSIBILITY

The report management procedure must define the circumstances under which a report will be deemed inadmissible;

5. PLANNED INTERNAL INVESTIGATIONS

Internal investigations must be properly planned, with a clear timeline to prevent undue delays that could exceed the designated time frame. The plan should define:

A. the scope of the investigation;
B. sources of evidence and required documentation;
C. the persons involved and those who should be interviewed.

6. EVIDENTIARY LIMITS

The collection of evidence in internal investigations must respect the evidentiary limits and, in any case, must respect the fundamental rights and principles recognised in the Charter of Fundamental Rights of the EU, as well as the provisions of national law and the internal procedures and protocols approved by the organisation.

7. MINIMIZING DOCUMENT REQUESTS AND REMINDING CONFIDENTIALITY

Not requesting documentation from departments of the organisation if that data can be obtained from open sources (for instance, an appointment of a civil servant published in an official gazette), also reminding the persons interviewed or the departments from which the information and/or documentation must be requested of the confidentiality obligations and the consequences that a breach of confidentiality may entail.

8. EVIDENCE COLLECTION RATIONALE IN REPORTS

The investigation report must include a rationale for the actions and verification methods used to collect evidence.

9. INTERVIEW PLANNING AND DOCUMENTATION

It is necessary, at the investigation planning stage, to determine the criteria for deciding which persons should be interviewed and in what order, as well as foreseeing the conditions of discretion for doing so and how the interview should be documented and recorded. It is advisable for it to be carried out by two investigators.

10. STRUCTURE OF THE FINAL INVESTIGATION REPORT

The report concluding the investigation must include: how the investigation was initiated, the objectives of the investigation, actions taken and individuals involved, assessment of the accuracy of the facts, and conclusions and recommendations for resolving the reported violation.

11. ENSURING OBJECTIVITY AND CLARITY IN REPORTS

The final report must be objective, impartial, clear, and precise.

12. MANAGING CONFLICTS OF INTEREST IN FOLLOW-UP

The follow-up procedure must include mechanisms for identifying, managing, and mitigating conflicts of interest among those responsible for handling reports.

13. RECOMMENDATIONS FOR ORGANISATIONAL IMPROVEMENT

The report management procedure must allow for the possibility of issuing recommendations to determine the treatment that detected situations of bad practices and lack of professionalism (wrongdoing) deserve and to be included in processes of continuous improvement of the organisation.

14. EXTENSION OF INVESTIGATION DEADLINES

If an investigation cannot be completed within the initial three-month period, an additional three-month extension may be granted. However, this extension must be approved before the first period ends, justify the reason for the delay, and specify the pending actions to be completed.

15. PROMOTING A CULTURE OF WHISTLEBLOWING

The competent authorities need to promote a culture of whistleblowing.

16. HANDLING EARLY EXTERNAL REPORTS

Transposition laws must clarify how to handle cases where a whistleblower reports externally before the internal investigation's three-month period has expired. This must align with the recommendations of the EU Commission expert group.

17. SANCTIONS FOR BREACHES OF CONFIDENTIALITY

Dissuasive and effective sanctions for non-compliance with the confidentiality requirement that specifically address the breach of this provision of the Directive. Therefore, in the case of a breach of confidentiality and duty of secrecy, it will be necessary to consider the offences typified in the transposition laws of the Member States. In the case of the Spanish transposition Law[46] , some offences have been typified as serious or very serious when:

A. the violation of the confidentiality and anonymity guarantees provided for in the Law, and in particular any action or omission tending to reveal the identity of the reporting person when they have opted for anonymity, even if the effective disclosure of this does not occur.

B. the violation of the duty to maintain secrecy on any aspect related to the report. The mention that this rule makes about the training of personnel with respect to confidentiality is relevant, given that the violation of the duty of secrecy, confidentiality and anonymity can constitute, as has already been mentioned, specific offenses.

[46] Law 2/2023, of February 20, regulating the protection of persons who report regulatory breaches and the fight against corruption.

Data protection

Chapter 3

Open the whistle

DATA PROTECTION

Chapter 3

3.1 THE ROLE OF DATA PROTECTION IN WHISTLEBLOWING SYSTEMS

Depending on the **type of reporting,** part of the **whistleblowing process** may involve the collection, use, and disclosure of **personal data,** placing it at the intersection of data protection and whistleblower **protection frameworks**. Ensuring that data protection principles are upheld while safeguarding whistleblowers' confidentiality and rights is essential to maintain trust and legal compliance. Data protection i**s not merely a regulatory obligation—it is a tool designed to support,** serve, and address the needs of all parties involved in the whistleblowing process. Far from being a hindrance to organisational workflows, robust data protection frameworks **provide clarity and structure,** ensuring that whistleblowers feel confident in reporting misconduct and in seeking help from support services, while also safeguarding the interests of the organisations receiving and handling such reports. When implemented thoughtfully, **data protection measures can foster** a culture of trust, enhance transparency, and ensure the integrity of internal reporting systems.

The GDPR (General Data Protection Regulation), as the cornerstone of data protection in the European Union, establishes the legal framework for processing personal data and balancing the rights and obligations of all stakeholders (**See chapter 1** to read about the difference between anonymity and confidentiality). The specific challenges of processing sensitive and personal data in whistleblowing contexts underscore the importance of aligning data protection strategies with the requirements of Directive on whistleblower protection. On a national level, frameworks for data protection in whistleblowing systems require meticulous planning and strategic alignment with national legal and cultural contexts.

The United Nations (UN) underscores the importance of protecting whistleblowers from retaliation as a cornerstone of transparency and accountability[47]. Whistleblowing mechanisms must prioritize the confidentiality of individuals to prevent any form of reprisal. This includes designing secure reporting channels, ensuring anonymity, and adopting technologies such as encryption to protect sensitive data. The **UN's "Protection Against Retaliation"** policy illustrates the critical role of data security in fostering a culture where individuals feel safe to report wrongdoing without fear of personal or professional harm.

[47] In this regard see: https://www.un.org/en/ethics/protection-against-retaliation/index.shtml#:~:text=The%20UN's%20protection%20against%20retaliation,by%20any%20person%20that%20is

3.2 MAIN CONCEPT AND KEY PRINCIPLES OF DATA PROTECTION

The interplay between the **General Data Protection Regulation** and the **Whistleblower Directive** 2019/1937/EU establish the legal framework to ensure that personal data is handled lawfully, ethically, and transparently. When **data protection principles** are embedded in the design of whistleblowing mechanisms, they enhance their credibility and ensure compliance with both **legal and ethical** standards.

3.2.1 Why is data protection essential for whistleblowers protection?

A. **safeguarding personal**, sensitive, and confidential information from misuse, theft, unauthorised access, etc;
B. **it preserves individual privacy** by ensuring control over personal data, reducing the risk of harm or exploitation;
C. **preventing identity theft** and fraud is a key benefit, as breaches exposing sensitive information can have devastating consequences. Businesses also gain trust by prioritizing data protection, which strengthens relationships with customers and partners of data protection, as non-compliance can lead to severe fines and reputational damage.

Beyond these practical benefits, **data protection is an ethical responsibility,** fostering fairness and transparency in how information is handled. In an interconnected world, robust data security also mitigates cybersecurity threats, by prioritizing data protection, individuals and organisations create a safer and more trustworthy.

Ch. 1 >

3.2.2 Key Principles of Data Protection

The principle of lawfulness, fairness, and transparency mandates that data processing should adhere to legal standards and be conducted transparently to maintain trust. Organisations should clearly communicate the purposes of data collection to data subjects, ensuring that their rights are understood and upheld. In short the principles laid down in Article 5 of the GDPR[48] are the starting point to ensure compliance with data protection rules and guarantee a fair, transparent and secure environment for data processing operations:

A. the **principle of lawfulness, fairness, and transparency** underscores the importance of processing personal data in a manner that complies with the law and respects the rights of the individuals concerned. In the context of whistleblowing, lawfulness mandates that organisations ensure a legal basis for processing the data, such as compliance with a legal obligation or the pursuit of legitimate interests, such as investigating misconduct. Data should also be processed in a fair

[48] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

manner, providing for transparency, which would require organisations to inform whistleblowers about how their data will be collected, used, stored, and potentially shared, ensuring that they understand the implications of their disclosure;

B. the purpose **limitation principle** dictates that personal data collected through whistleblowing channels must only be used for the specific purposes for which it was gathered. For example, if a whistleblower reports allegations of fraud, the information provided must be used strictly for investigating the reported issue and not for unrelated purposes such as, for example, evaluating the whistleblower's job performance. This principle protects against the misuse of data and ensures that the rights of whistleblowers and other individuals involved are not unjustly compromised;

C. **data minimization** is a key principle that emphasizes the need to collect only the data that is strictly necessary for the investigation of the reported matter. Excessive data collection not only increases the risk of breaches or misuse but can also lower the trust whistleblowers place in the confidentiality of the reporting process. For instance, details about third parties or the identity of the whistleblower should only be disclosed when absolutely essential to the investigation and in compliance with applicable laws;

D. the **principle of accuracy** ensures that all personal data processed in the context of whistleblowing is correct and up to date. Inaccurate data can lead to unjust outcomes, such as baseless accusations or the wrongful conclusion of investigations. Organisations must implement procedures to verify the accuracy of the information provided by whistleblowers and to rectify inaccuracies promptly if they are identified;

E. **storage limitation** requires that personal data be retained only for as long as necessary to fulfil the purpose for which it was collected. In whistleblowing cases, this means that data should be kept only for the duration of the investigation and any subsequent legal or administrative proceedings. Retaining data indefinitely could expose individuals to undue risks, such as breaches or misuse, and would contravene established data protection principles;

F. the **principles of integrity and confidentiality** under the GDPR are of paramount importance, for example when in the case of whistleblowers highly sensitive information may be provided, and it is the responsibility of organisations to ensure that this data is secure. Robust measures such as encryption, access controls, and secure reporting channels are essential to prevent unauthorised access, data breaches, and other risks that could compromise the confidentiality of whistleblowers or the integrity of investigations;

G. the **principle of accountability** requires organisations to demonstrate compliance with data protection laws in their handling of whistleblowing cases. This entails maintaining records of data processing activities, conducting data protection impact assessments for whistleblowing systems, and ensuring that any third parties involved in the investigation, such as external auditors or investigators, adhere to relevant data protection regulations. Regulation (EU) 2016/679 accounts for the confidentiality requirements set in other legal acts at both national and EU level, and foresees that only the type of data should be accounted for, and not the actual data itself.

In addition to these core principles, whistleblower protection must also address specific considerations such as anonymity, the balancing of rights between whistleblowers and implicated parties, and cross-border data transfers. Providing anonymous reporting channels aligns with the objective of protecting whistleblowers from retaliation. At the same time, organisations must balance the confidentiality of whistleblowers with the rights of implicated individuals to access information concerning allegations made against them, ensuring this is done in accordance with legal requirements. When whistleblowing involves international matters, organisations must ensure that any cross-border transfers of data comply with applicable regulations, such as the General Data Protection Regulation in the EU. It is crucial to adhere to these principles so that organisations can protect the rights of all parties involved, ensure compliance with legal frameworks, and foster a culture of accountability and transparency in whistleblowers protection systems, and help cultivate trust.

3.3. LEGAL BASIS FOR LAWFUL PROCESSING OF PERSONAL DATA

Article 6 GDPR

Organisations involved in whistleblowing processes must identify a lawful basis for processing personal data as outlined in Article 6 of the GDPR[49]. The legal bases for processing include consent, contractual necessity, legal obligation, vital interests, public interest, and legitimate interests:

A. **consent**, personal data processing is lawful when the data subject has freely given specific, informed, and unambiguous agreement for their data to be processed for a particular purpose. Consent must be clear, explicit (if processing sensitive data), and easily withdrawable at any time;

B. **contractual obligation** basis applies when processing is required to fulfil a contract to which the data subject is a party or to take pre-contractual steps at the request of the data subject. This ensures that data processing is directly linked to the performance or preparation of a contractual obligation (Whistleblowers protection can be part of the provisions of any contract);

C. **legal obligation** is lawful when it is necessary to comply with a specific legal requirement imposed on the data controller. This basis is typically used when legislation mandates the retention, reporting, or sharing of data (Under legislative acts, such as Directive and national law, whistleblowers protection is subject to legal obligations applicable for organisations);

D. **vital interests** basis justifies processing when it is necessary to protect the life or physical safety of the data subject or another person. This basis is often relied upon in emergencies, such as medical situations, where consent cannot be obtained;

E. **public interest** or official authority basis applies when processing is necessary for carrying out a task in the public interest or in the exercise

[49] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

of official authority vested in the data controller. This is commonly used by public bodies or organisations operating under statutory or governmental mandates, while it should be explicitly stated in the particular legal act;

F. **legitimate interests**, processing is lawful when it is necessary to achieve the legitimate interests of the data controller or a third party, provided these interests are not overridden by the rights and freedoms of the data subject. This basis requires a careful balancing test to ensure that the processing does not unfairly impact the data subject's privacy (While the choice of the most appropriate legal basis is in the hands of organisations, when possible it is recommended to rely on the other legal basis provided in Article 6 of the GDPR).

In summary, the lawful processing of personal data under Article 6 of the GDPR is essential for ensuring compliance and fostering trust in whistleblowing mechanisms. Organisations must carefully determine and document the appropriate legal basis while balancing the rights of data subjects and requirements under Directive.

Article 9 GDPR

Special categories of personal data, including information related to racial or ethnic origin, political opinions, religious beliefs, health, or sexual orientation, are subject to heightened protections under Article 9 of the GDPR[50]. These types of data are considered sensitive and require specific conditions to justify their processing. Explicit consent remains a primary basis for processing sensitive data, but organisations must ensure that such consent is freely given and well-documented.

[50] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

GENDER BOX

By integrating gender-sensitive policies into **data protection frameworks**, whistleblowing systems can become safer and more effective, encouraging more individuals — especially women—to come forward without fear of retaliation or exposure. These measures are essential to ensuring that gender-based misconduct reports are securely handled and whistleblowers' identities remain protected, especially when there are power dynamics that could influence the process. It is recommended to:

A. emphasize how security systems prevent retaliation in gender-based cases, ensuring that reports are protected from being accessed by individuals in the same workplace hierarchy, such as supervisors or colleagues, to avoid potential retribution;

B. ensure that platforms claiming anonymity truly protect the whistleblower's identity, particularly in cases involving gender and intersectional power imbalances (e.g., employer-employee, professor-student, government-citizen);

C. provide explicit information on how digital security measures (e.g., Tor, zero-knowledge proofs, IP masking) protect whistleblowers reporting gender-based misconduct;

D. developing online platforms and hotlines for reporting corruption offer the advantage of allowing individuals to make disclosures from home and, in some cases, anonymously. This way of reporting **can be particularly convenient to report gender violence** linked to corruption and sextortion.

These measures are essential to ensuring that gender-based misconduct reports are securely handled and whistleblowers' identities remain protected, especially when there are power dynamics that could influence the process.

Confidentiality Protocols for Gender-Based Reports:

A. specify additional confidentiality protections for whistleblowers reporting gender-based misconduct, including measures to prevent indirect identification through case details;

B. detail how reports involving gender-based violence (GBV) will be securely stored and segregated from general misconduct reports to minimize exposure;

C. clarify who has access to reports and how identity protection is enforced, ensuring no unauthorised individuals (e.g., colleagues or direct superiors) can access sensitive data;

D. confidentiality is key to maintaining the integrity of gender-based misconduct reporting and protecting whistleblowers from potential harm.

Other legal bases for processing sensitive data include compliance with legal obligations, the necessity of processing for substantial public interest, and the protection of vital interests. For instance, whistleblowing cases involving allegations of discrimination may require the processing of sensitive data to substantiate claims or comply with anti-discrimination laws. Organisations must exercise caution and implement additional safeguards when handling such data to mitigate risks and ensure compliance.

Data subject rights under regulation (EU) 2016/79

The GDPR grants data subjects a range of rights designed to empower individuals and provide greater control over their personal data. Among them are:

A. the **right of access**, which allows individuals to obtain detailed information about the processing of their data, including the purposes, categories, recipients, and retention periods;
B. the **right to rectification**, which ensures that inaccurate or incomplete data can be corrected promptly, enhancing the accuracy and reliability of processed information;
C. the **right to request the erasure of data** under specific circumstances, such as when the data is no longer necessary for its original purpose or when consent is withdrawn. However, this right is not absolute and must be balanced against the need to retain data for legal or investigative purposes;
D. the **right to restrict processing**, which allows individuals to limit the scope of data processing activities, particularly during disputes over accuracy or the legality of processing;
E. **data portability**, which enables individuals to receive their data in a structured, commonly used, and machine-readable format and transfer it to another controller. This right enhances individual autonomy and facilitates competition among service providers;
F. **the right to object**, which allows individuals to challenge data processing activities based on legitimate interests or public interest grounds. Organisations must assess such objections carefully and provide clear justifications for continuing or ceasing processing activities.

Each country determines the specific procedures for data subjects to exercise their rights under Articles 15-22 of the GDPR[51], this usually includes a request to the data controller for exercising their rights. **National legislation determines whether such requests should be submitted** electronically, in writing, or both, or through a specific for the organisation method, which should not create additional difficulty for data subjects, nor exceed disproportionately the administrative burden for the controller.

3.6. INTERPLAY BETWEEN PERSONAL DATA PROTECTION LEGAL FRAMEWORK AND DIRECTIVE 2019/1937/EU

While the GDPR provides data subjects with a spectrum of rights, its interplay with other legislation should always be kept in mind. **When data subjects are viewed as whistleblowers** under Directive, **they can still exercise each of their rights under the GDPR**, however organisations may

[51] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

refuse to carry out requests from data subjects to exercise their rights, or directly refuse, when this would be in violation of the legal requirements for the protection of whistleblowers under both Directive and national law. While the GDPR sets requirements and deadlines related to the deletion of data, in this case the person submitting the report, or simply upon completion of the purpose for which the data was collected, the Regulation is still considered as lex generali. To this end where there are different retention periods for different types of data in national legislation, they are applied over the ones set by the GDPR. Additionally, entities may still use **"legitimate interest"**, however, when doing it should be proved by enough evidence.

Both frameworks share common objectives of fostering transparency and accountability while safeguarding the rights of individuals. Confidential handling of whistleblowing reports is a fundamental requirement under the Directive and the GDPR. Both frameworks mandate that only the data necessary for achieving the purposes of the reporting mechanism should be collected and processed. This reduces risks associated with over-collection and ensures compliance with the principle of purpose limitation.

Data must be retained only for as long as necessary to investigate and resolve reported issues. For instance, in **Italy**, the applicable national law provides that reports cannot be used beyond what is necessary to adequately follow up on them. The identity of the reporting person and any other information from which such identity can be deduced, directly or indirectly, cannot be revealed, without their express consent, to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data pursuant to Articles 29 and 32, paragraph 4, of Regulation (EU) 2016/679[52] (art. 12.1). It is also provided that personal data that are manifestly not useful for the processing of a specific report are not collected or, if collected accidentally, are deleted immediately (art. 13.2). Internal and external reports and the related documentation are kept for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure.

Public and private bodies define their own model for receiving and managing internal reports, identifying technical and organisational measures suitable for guaranteeing a level of security adequate to the specific risks arising from the processing carried out, on the basis of a data protection impact assessment. Furthermore, **the Italian data protection legislation** includes a specific provision to protect the confidentiality of the whistleblower's identity (art. 2-undecies in Legislative Decree no. 196 of 30 June 2003. This article was introduced with Legislative Decree no. 101 of 10 August 2018, to comply with EU Regulation no. 2016/679). The aforementioned provision establishes that in the context of a report, the affected subject, presumed author of the violation, with reference to their personal data processed by the Administration, cannot exercise the rights

[52] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

provided for in Articles 15 to 22 of Regulation (EU) No. 2016/679, since the exercise of such rights could result in damage to the protection of the confidentiality of the identity of the whistleblower. The law provides for the possibility for the affected person to request from the Data Protection Authority checks on the conformity of the processing of their data. The Data Protection Authority provides feedback on the relative outcome.

By aligning data protection strategies with the requirements of the Whistleblower Directive:

A. **organisations** can create integrated systems that respect individual rights while supporting effective governance and compliance. Whistleblowers feel confident in coming forward, knowing their personal data will be treated with the utmost care;
B. **public trust** in reporting systems is strengthened;
C. **regulators** and organisations must work collaboratively to ensure seamless implementation, leveraging tools such as standardized reporting protocols, clear data retention guidelines, and accessible anonymisation techniques.

3.8 DATA PROTECTION BY DESIGN AND BY DEFAULT IN INTERNAL REPORTING CHANNELS

Organisations can build robust whistleblowing systems that align with the principles of data protection by design and by default.

3.8.1 What is data protection by design?

Internal reporting channel: Embedding security measures and privacy considerations into the development of reporting mechanisms. For example, systems should include features such as encrypted communication channels, role-based access controls, and audit logs to ensure confidentiality and accountability. Data minimization should guide the design of reporting forms and workflows, ensuring that only essential information is collected during the initial report. Organisations should also implement procedures for verifying the accuracy and relevance of collected data while safeguarding the anonymity of whistleblowers. Example for this would be the development of internal mechanisms allowing for cross-check of specific types of data, without revealing the identity of the whistleblower, in order to prove the validity of the claims made in the submitted reports. There are already existing software solutions (including softwares used by data analysts) which allow for different databases (specific departments, HR, etc.) to cross-check such information in anonymous format.

A case study from Italy: The deployment of software systems incorporating robust encryption to guarantee confidentiality across external reporting channels is a benchmark for effective data protection by design. An example is Globaleaks, which creates an identifier for each whistleblower, enabling an asynchronous and secure communication with the reporting channel. Such

a practice ensures that neither party can access unnecessary personal data, thus fulfilling the principle of data minimization.

3.8.2 What is data protection by default?

The need for organisations to process only the data necessary for specific purposes. Internal reporting systems must automatically apply the highest privacy settings and limit data access to designated personnel. Regular evaluations of system configurations and practices ensure that these principles are consistently applied and updated to address emerging risks and regulatory changes. To strengthen data protection, organisations should adopt innovative technologies such as automated compliance checks, real-time anomaly detection in data flows, and encrypted storage solutions (see **Chapter 1** for further information). Engagement with employees through workshops or training on data protection and internal reporting systems can bridge the gap between technology and practical application. This holistic approach ensures that staff at all levels understand their responsibilities, fostering a culture of proactive data protection.

3.9. DATA PROTECTION IN EXTERNAL REPORTING CHANNELS

External reporting channels, such as those operated by regulatory bodies, face additional challenges in balancing transparency with data protection. **Secure communication channels** are essential to protect the integrity of reports and prevent unauthorised access to sensitive information. Organisations operating external channels should establish clear policies **outlining the handling of personal data,** including procedures for verifying the authenticity of reports and protecting whistleblowers' identities.

Transparency is key; Anonymity options should be available to whistleblowers, with mechanisms for secure follow-up communication. The protection provided to whistleblowers falls within the legitimate purposes under the GDPR, providing information to a person subject of a submitted report while the investigation is ongoing, may corrupt the investigation itself by leading to the identification of the whistleblower. The use of secure and auditable systems can ensure accountability and compliance with data protection requirements. Regulatory bodies should also consider implementing multi-layered access controls and robust encryption protocols to secure sensitive information. Periodic third-party audits of these systems provide an additional layer of assurance that data protection principles are upheld. To ensure public confidence, external reporting channels must also emphasize fairness and impartiality. Such measures demonstrate a commitment to both data protection and accountability, strengthening trust in external reporting systems

3.9.1 Good Practices from Italy

To comply with all the above mentioned GDPR requirements, in **Italy**, the Legislative Decree 24/2023 provides that reports cannot be used beyond what is necessary to adequately follow up on them. The identity of the reporting person and any other information from which such identity can be deduced, directly or indirectly, cannot be revealed, without their express consent, to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data pursuant to Articles 29 and 32, paragraph 4, of Regulation (EU) 2016/679[53] (art. 12.1). It is also provided that personal data that are manifestly not useful for the processing of a specific report are not collected or, if collected accidentally, are deleted immediately (art. 13.2).

Internal and external reports and the related documentation are kept for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure, according to a specific provision of **the Italian data protection legislation** (art. 2-undecies in Legislative Decree no. 196 of 30 June 2003, introduced with Legislative Decree no. 101 of 10 August 2018).

3.9.2 Mitigating Reputational Risks

External reporting channels also face heightened reputational risks when sensitive information becomes public, as emphasized by Italian respondents. Employee disclosures via social media, for instance, can significantly harm a company's or public authority's reputation. Implementing strict policies on public disclosure and promoting secure external reporting channels can mitigate these risks. Article 11-ter of the Italian Code of Conduct underscores this issue, demonstrating the need for alignment between national laws and the Directive's provisions. To counter reputational risks while adhering to the Directive's principles, organisations can offer multiple secure and official reporting avenues, including anonymous hotlines and encrypted online platforms. These channels can pre-empt whistleblowers from resorting to social media, thereby maintaining confidentiality and limiting reputational damage.

3.9.3 Expertise and Training

Feedback from Spanish interviews highlights the critical importance of expertise in data protection. Organisations should ensure that personnel operating external reporting channels are adequately trained and possess a thorough understanding of GDPR requirements. Regular workshops and certification programmes for Data Protection Officers (DPOs) and other relevant staff can bolster compliance and foster a privacy-first culture. By implementing these measures, external reporting channels can meet the

[53] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

dual objectives of promoting transparency and safeguarding the rights of all parties involved, fostering trust and legal compliance.

3.10. TECHNICAL AND ORGANISATIONAL MEASURES

Implementing robust technical and organisational measures is essential to ensure compliance with the GDPR[54] and safeguard personal data. Encryption and pseudonymization are widely recognized techniques that enhance data security by rendering data unintelligible to unauthorised parties. Role-based access controls limit data access to authorised personnel, reducing the risk of unauthorised disclosures.

Organisations must develop and implement comprehensive data protection policies that outline roles, responsibilities, and procedures for handling personal data. Regular training and awareness programmes for employees ensure that all stakeholders understand their obligations under the GDPR and whistleblower protection frameworks. Periodic audits and risk assessments help identify vulnerabilities and ensure that security measures remain effective and up to date.

Incident response plans are important for addressing data breaches and minimizing their impact. Organisations must establish clear protocols for detecting, reporting, and mitigating breaches, as well as notifying affected individuals and authorities where required.

3.11. DATA PROTECTION BY DESIGN AND BY DEFAULT IN PUBLIC DISCLOSURE

Public disclosure presents unique challenges in balancing data protection with the need for transparency and accountability. How organisations maintain their obligations for whistleblowers protection in these cases is essential. Public disclosure in fact, represents the most sensitive form of whistleblowing, where the potential for reputational harm and legal implications is highest. Under Directive, public disclosure is considered a last resort, permissible only when internal and external reporting channels have been exhausted or are deemed ineffective. Before disclosing information to the public, organisations (either in the role of external or internal reporting channels) must carefully assess whether the disclosure aligns with GDPR principles and serves the public interest. Explicit consent should be obtained whenever possible, particularly when sensitive personal data is involved.

3.11.1 The Role of Data Protection in Public Disclosures

In the context of public disclosures, organisations and whistleblowers must carefully navigate the fine line between transparency and reputational

[54] In this regard see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

harm. Redaction protocols play a critical role in protecting privacy during public disclosures. Organisations must remove or obscure personal data that is not essential to achieving the purpose of the disclosure. This ensures compliance with the principle of data minimization while safeguarding the rights of individuals. The aforementioned GlobaLeaks software from **Italy** exemplifies how technology can support public disclosures. By anonymising and encrypting communications, such platforms allow whistleblowers to share information securely, reducing the risks associated with unregulated public disclosures. Incorporating such technology into public disclosure frameworks can ensure compliance with the Directive while maintaining the whistleblower's trust.

From **Italy** a concern has been raised about the potential misuse of public disclosures via social media. When whistleblowers bypass formal reporting mechanisms and disclose sensitive information on open platforms, it not only jeopardizes their confidentiality but also poses significant risks to corporate or institutional reputation.

Organisations must inform employees about the legal boundaries of public disclosures. Article 11b of the Italian Code of Conduct, for example, addresses the careless use of social networks and emphasizes the importance of adhering to structured reporting mechanisms. Complementing these measures with accessible and robust internal and external channels can reduce the likelihood of whistleblowers resorting to public platforms. However, in Italy there is still a misalignment between the provisions of the Code of Conduct and Legislative Decree 24/2023 on whistleblowing. The latter explicitly recognises the possibility of public disclosure under certain conditions, a nuance that is not adequately reflected in the Code. At the same time, the lack of alignment between the Code of Conduct and the current legislative framework creates confusion regarding the recipient of internal reports, as it still incorrectly identifies the hierarchical superior instead of the Responsible for the Prevention of Corruption and Transparency.

3.11.2 How to enhance security in Public Disclosures?

To align public disclosures with data protection principles, organisations and oversight bodies must develop clear guidelines and protective measures. Spanish stakeholders have highlighted the importance of safeguarding the whistleblower’s identity even in public disclosures.

The **Bulgarian** perspective emphasizes the importance of limiting access to reports to essential personnel. Applying the same principle to public disclosures, oversight bodies can redact sensitive information that is not critical to the public interest, balancing transparency with data protection.

To prevent data mismanagement when a public disclosure is made, we recommend that regulatory bodies must implement stringent measures to prevent the mishandling of data, such as:

A. establishing protocols for verifying the accuracy of reported information
B. documenting all actions taken in response to the disclosure.

Transparent communication about these processes reassures stakeholders and reinforces trust in the system.

3.12. DATA PROTECTION AND INFORMATION CENTRE(S) ORGANISED BY CIVIL SOCIETY: AN OPEN ISSUE

Article 20 of Directive[55] recognises the role of "information centres" as support services that civil society can organize and make available to help potential whistleblowers during the phase of ethical dilemmas and general doubts about the functioning of the system. The law provides that this role can nalso be fulfilled by dedicated institutions.

To fulfil this role (**see Chapter 4**), such information centres necessarily come into contact with, manage, and store personal data, as well as other sensitive information.

Ch. 4>

In this regard, the initial provision No. 89 of the Directive states that information centres "**are bound by a duty to maintain the confidentiality of the information received**".

However, the Directive does not provide further specifics on how to comply with this duty, whether these centres should be equated with reporting institutions, or whether special conditions should apply. **The Directive remains vague on this point**. This gap has not been sufficiently addressed in the regulations of various countries, particularly given that, with rare exceptions, such support services are not yet widely practiced across Europe.

In the absence of specific guidelines on data processing practices, **there is a risk that support services may be prevented from processing data**, thus limiting their ability to function (and potentially jeopardizing their ability to operate at all), while also restricting potential whistleblowers' access to support.

National regulations, or guidelines provided by the relevant authorities for whistleblowing, should aim to fill this gap by establishing clear data processing protocols that enable whistleblowers to receive support, while requiring information centres to implement strong encryption systems for receiving, storing (for a limited period), and sharing data among operators, best ensuring the protection and confidentiality of the whistleblower's information. As it is stipulated in Recital 74 of Directive, staff members of the competent authorities who are responsible for handling reports should be professionally trained, including on applicable data protection rules, in order

[55] In this regard see: https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng

to handle reports and to ensure communication with the reporting person, as well as to follow up on the report in a suitable manner.

OPEN GOVERNMENT BOX

Robust data protection strategies are paramount for a plethora of stakeholders, such as whistleblowers, managers of reporting channels, entities offering support to potential whistleblowers such as CSOs, and stakeholders who have a role as public disclosure channel, such as journalists and media. These strategies should include secure mechanisms for handling sensitive information to safeguard the identity and interests of whistleblowers. **Cross-sector collaboration** with involvement of national regulators, Data Protection Officers, and policymakers can be decisive in the development of innovative **data protection solutions tailored to diverse whistleblowing scenarios, especially to address the complexities of public disclosures**. Joint efforts can harmonise national laws with the Directive's provisions, developing clear guidelines on the ethical use of data to help all stakeholders maintain transparency while respecting privacy.

One increasingly critical issue to be addressed within an Open Government framework is the **handling of sensitive and personal data by advisory and support entities** - both civic and institutional - as recognised by Directive. The Directive itself (in initial provisions 89 and 90) mandates that these entities ensure effective data processing, though it does not provide further specifics.

Support and advisory services, in their role of guiding potential whistleblowers, inevitably come into contact with sensitive data. Their purpose is not merely to provide generic, decontextualized information, but rather to assist individuals in navigating the proper reporting channels in a meaningful way. A purely neutral, detached approach would fail to meet the needs of potential whistleblowers.

This issue should be openly discussed within an Open Government setting, through the development of clear guidelines, by organizing joint discussions involving data protection authorities, representatives of support organisations (both civic and institutional), and whistleblowing regulatory bodies.

The goal should be to strike the right balance between two key needs: ensuring that potential whistleblowers receive meaningful guidance (which may require some level of data processing by support services) while also safeguarding their personal data.

For example, discussions should establish:

A. clear retention policies, including a maximum storage period for sensitive data;
B. secure, confidential methods for data exchange between potential whistleblowers and support services;
C. defined communication protocols among advisors within the same service.

A restrictive interpretation that prioritises privacy above all else could unintentionally undermine the very interests of potential whistleblowers by limiting their ability to seek effective guidance.

FINAL RECOMMANDATIONS

The Konrad Adenauer Foundation (KAF) throughout its work on various projects and policies emphasizes that comprehensive legal frameworks (similar to the GDPR[56]) are essential for fostering transparency while safeguarding individual rights, clearly defining the scope and boundaries of whistleblowing activities. KAF advocates for mechanisms that uphold the principle of proportionality in data handling balancing the need to investigate reported misconduct with the right to privacy of all individuals involved. They also highlight the significance of public awareness campaigns to educate citizens and organisations about their rights and responsibilities within whistleblowing frameworks. Some practical tips for the implementation of data protection policies have been listed[57]:

1. ESTABLISHING INDEPENDENT OVERSIGHT BODIES

The establishment of independent oversight bodies to monitor the implementation of whistleblowing mechanisms, as it is defined by the applicable national legal framework.

2. AUTHORITY OF INDEPENDENT BODIES

These bodies should have the authority to investigate complaints, review data protection practices, and ensure compliance with legal standards, when it refers to independent authorities that receive complaints through an external channel (or their internal channel).

3. IMPORTANCE OF TRAINING PROGRAMMES

Training programmes for both public and private sector employees are crucial to build awareness of whistleblowing protocols and data protection principles.

4. HANDLING SENSITIVE REPORTS AND CONFIDENTIALITY

Employees must be equipped to recognize the importance of confidentiality, securely handle sensitive reports, and avoid unauthorised disclosures.

5. GOOD PRACTICES TO STRENGTHEN COMPLIANCE

Overall, here are several good practices that organisations can follow to strengthen their compliance and foster trust:

[56] In this regard see: https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_47778_2.pdf/c2a538a2-ed3d-1aa7-b2ae-2736329c8a66?version=1.0&t=1539649646584

[57] In this regard see: https://www.kas.de/en/web/rspno/veranstaltungsberichte/detail/-/content/transparenz-und-rechenschaftspflicht

5.1. DEVELOPING DETAILED WHISTLEBLOWING POLICIESRMARE IL PERSONALE COINVOLTO NELLE DIVULGAZIONI PUBBLICHE

Organisations should develop detailed policies that outline the purpose, scope, and procedures of their whistleblowing systems. These policies must address data protection requirements, including data collection, storage, processing, and retention. By making these policies accessible to all stakeholders, organisations demonstrate transparency and accountability.

5.2. APPOINTING A DATA PROTECTION OFFICER (DPO)

Appointing a qualified Data Protection Officer is critical for ensuring ongoing compliance with GDPR and the Whistleblower Directive. DPOs can provide guidance on handling personal data, conduct audits, and serve as a point of contact for data subjects and supervisory authorities.

5.3. TAILORING TRAINING PROGRAMMES TO STAKEHOLDERS

Training **programmes** should be tailored to the needs of different stakeholder groups, including employees, managers, and external service providers. These programmes should emphasize the importance of confidentiality, data minimization, and the rights of data subjects. Scenario-based training can help employees understand how to handle sensitive whistleblowing cases effectively.

5.4. IMPLEMENTING SECURE REPORTING CHANNELS

Organisations should implement secure and user-friendly reporting channels that allow whistleblowers to submit information confidentially. Multi-factor authentication and encrypted communication protocols can enhance the security of these systems. Additionally, organisations should test these systems regularly to identify and address vulnerabilities.

5.5. PERIODIC MONITORING AND AUDITING

Periodic monitoring and auditing of whistleblowing systems help ensure compliance with data protection requirements. Organisations should maintain detailed records of data processing activities, including justifications for data collection and retention. Audits can identify gaps in compliance and provide opportunities for continuous improvement.

5.6. ENGAGING WITH REGULATORY BODIES

Engaging with national data protection authorities and other regulatory bodies can help organisations stay informed about changes in legislation and best practices. Collaboration also facilitates the resolution of complex cases, such as those involving cross-border data transfers or conflicts between national and EU regulations.

5.7. UTILIZING INNOVATIVE TECHNOLOGIES

Innovative technologies, such as artificial intelligence and machine learning, might enhance the efficiency and security of whistleblowing systems. For example, AI-powered tools can detect patterns of misconduct, identify data breaches, and support anonymisation processes. However, organisations must ensure that these technologies comply with GDPR and

other applicable regulations.

5.8. ESTABLISHING METRICS FOR EFFECTIVENESS

Organisations should establish metrics to evaluate the effectiveness of their whistleblowing systems, including the resolution rate of reported cases, the satisfaction levels of whistleblowers, and the organisation's overall compliance with data protection standards. Regular reporting on these metrics can build trust among stakeholders and highlight areas for improvement (See **chapter 5** for further information).

5.9. FOSTERING CONTINUOUS IMPROVEMENT

Data protection is an ongoing process that requires organisations to adapt to changing legal, technological, and societal landscapes. By fostering a culture of continuous improvement, organisations can ensure that their whistleblowing systems remain effective, secure, and compliant with evolving standards. By incorporating these strategies/good practices, organisations, as well as national governments, can establish whistleblowing mechanisms that are both legally compliant and practically effective. These systems not only encourage individuals to report misconduct confidently but also strengthen overall governance, enhance public trust, and contribute to a culture of integrity.

5.10. BALANCING PUBLIC INTEREST WITH PRIVACY RIGHTS

Balancing public interest with privacy rights requires a proportionality assessment, considering factors such as the severity of the reported issue, the potential impact of disclosure, and the availability of alternative solutions. Organisations must document their decision-making processes to demonstrate accountability and compliance with regulatory requirements such as internal registers, rules and procedures, codes of conduct as well as codes of ethics.

5.11. PRIORITIZING WHISTLEBLOWER CONFIDENTIALITY IN PUBLIC DISCLOSURES

Public disclosure mechanisms must prioritize maintaining whistleblower confidentiality unless explicit consent is provided. Organisations should establish clear and accessible processes for whistleblowers to express their preferences regarding disclosure and ensure these preferences are respected.

5.12. CONDUCTING RISK ASSESSMENTS BEFORE PUBLIC DISCLOSURE

For public disclosures, robust risk assessment frameworks should be implemented to evaluate the potential consequences of releasing information. This includes assessing the likelihood of harm to whistleblowers, the individuals implicated, or the public. When possible, anonymisation and pseudonymisation techniques should be applied to the data before disclosure.

5.13. USING AUTOMATED REDACTION TOOLS

The use of technological solutions, such as automated redaction tools, can streamline the preparation of data for public disclosure. These tools can detect and mask sensitive personal information consistently and efficiently, minimizing the risk of human error.

5.14. ESTABLISHING CRITERIA FOR PUBLIC DISCLOSURE

Organisations must also establish clear criteria for determining when public disclosure is appropriate. Factors to consider include the urgency of the issue, the availability of internal or external reporting mechanisms, and the potential benefits and risks of disclosure.

5.15. TRAINING STAFF INVOLVED IN PUBLIC DISCLOSURES

Finally, education and training programmes for staff involved in public disclosure processes are essential. These programmes should cover the legal and ethical aspects of data protection, the importance of balancing privacy with transparency, and the technical skills required to handle sensitive information.

Protection and support of whistleblowers

Chapter 4

Open the whistle

PROTECTION AND SUPPORT OF WHISTLEBLOWERS

Chapter 4

4. 1 PROTECTION PROVIDED BY DIRECTIVE 2019/1937/EU

The Directive provides comprehensive protection to individuals who report breaches of Union law, ensuring that a broad spectrum of people involved in work-related activities are safeguarded against retaliation. This protection extends beyond traditional employees and encompasses a wide range of individuals:

A. civil servants, as well as self-employed individuals such as freelancers and independent contractors (under Article 49 TFEU);
B. shareholders and non-executive board members;
C. Volunteers and trainees, whether paid or unpaid;
D. former workers;
E. facilitators—natural persons who assist whistleblowers confidentially. This includes legal advisers offering strategic guidance, union representatives advocating for whistleblowers, and other trusted intermediaries who help navigate the complexities of disclosure;
F. third parties who might suffer retaliation due to their connection with the whistleblower, including family members, colleagues, and even legal entities linked to the reporting person.

Notably, whistleblower protection **does not apply** to individuals who disclose information directly to the press, except in cases where national laws establish specific protections for freedom of expression and information (Article 15.2). As a result, **journalists are excluded from the Directive's protections**.

In **Bulgaria** attempts are being made to incorporate aspects of the SLAPP concept and whistleblower protection legislation into the defence of cases against journalists. However, it would be useful to have clear **evidence** at the legislative level (EU and national law) and in practice, that "the protection of freedom of expression in Strategic lawsuits against public participation (SLAPP) cases should go hand in hand with the protection of whistleblowers". Based on this consideration, Protection **remains valid regardless** of the chosen channel, as long as the disclosure complies with the Directive's provisions. If **internal or external** mechanisms prove ineffective or if there is an imminent threat to the public interest, whistleblowers can make their concerns public without losing their **legal base** for protection.

However, different stakeholders **perceive internal channels** as **less secure than external ones**, particularly when reports conflict with an organisation's interests. Many fear retaliation. This concern **extends to personnel tasked with receiving and handling** reports, who - at least in **Italy** - often lack

independence from their organisations and do not enjoy the necessary safeguards that would enable them to pursue reports effectively.

4.1.2 What the whistleblower has to do to qualify for protection?

As anticipated, to qualify for protection under the Directive, **whistleblowers must meet specific conditions,** namely, that reports are made through appropriate channels and that reporting persons have a **reasonable belief** that the disclosed information is true. The **Directive** does not allow subjective evaluations of a whistleblower's motives for reporting a violation. Thus, "**good faith"** is not a relevant factor; instead, what matters is that the whistleblower **reasonably believes** that an offence has been committed or is likely to be committed. This concept, referred to as reasonableness, replaces the traditional good faith standard.

What constitutes a "reasonable belief"?

A. a **reasonable belief** is **based on objective, concrete elements, such as evidence or verifiable indications**, that lead the reporting person to believe that the facts presented are true. This means that even if the reported information later turns out to be incorrect, the whistleblower remains protected as long as they had legitimate grounds to consider it accurate at the time of reporting. This safeguard is crucial in encouraging individuals to come forward without fear of punishment for unintentional errors;

B. a whistleblower's **personal motive** for reporting is **irrelevant** to their protection. This principle is reaffirmed in **Recital 32 of the Directive** and reiterated in UNCAC Resolution 10/8 "Protection of Reporting Persons", paragraph 14. After 2019 there has been a **definitive shift from assessing a whistleblower's personal motives to evaluating the objective facts of the report itself**. The principle of reasonableness also plays a crucial role in preventing malicious reports (i.e., manifestly false claims) that could unfairly harm individuals or organisations. However, the European Convention on Human Rights (ECHR) continues to include good faith as a requirement for protection, which creates a clear conflict with the Directive.

What matters is that reports are made in the public interest or in the interest of the integrity of the public administration or private entity: the reasons that led the person to report, denounce or publicly disclose are irrelevant for the purposes of their protection.

Protection in anonymous reporting

To ensure protection, Whistleblowers must use the reporting channels described in Chapter 2.

Ch. 2>

The Directive acknowledges that anonymous reports can help build trust in whistleblowing systems. Whistleblowers who choose to report anonymously and later reveal their identity remain eligible for protection if they face retaliation (art.6.3). However, the treatment of anonymous reporting varies across the three countries involved in this project, and more in general across Europe.

Italian legislation does not provide for anonymous reports, except for the recognition of protection to anonymous whistleblowers who suffer retaliation. ANAC, which manages the **external channel,** treats anonymous reports as ordinary complaints until protection is invoked. If an anonymous whistleblower later faces retaliation, they are entitled to the same protections as non-anonymous whistleblowers **(Article 6, Legislative Decree 24/2023**). A key difference regarding anonymous reporting is that access to the report is considered permitted under specific conditions and limitations established by the Italian law. This is because anonymous complaints are treated as ordinary complaints under general legal provisions: a) documentary and defensive access (Articles 22 et seq. of Law no. 241/1990), and b) civic access (Articles 5 et seq. of Legislative Decree no. 33 of 2013).

Bulgaria does not formally regulate anonymous whistleblowing. However individuals who have submitted anonymous reports or publicly disclosed information about violations, and who are later **identified and subjected to retaliation**, **are entitled to protection (Article 10, Bulgarian Whistleblowing Act).**

Spain allows anonymous reporting and mandates **protection for whistleblowers who are later identified and subjected to retaliation** (**Article 7(3) for internal reporting and Article 17 for external reporting, Law 2/2023, February 20th**). Under Spanish law, violating the guarantees of confidentiality and anonymity constitutes a very serious infringement within the sanctioning regime. Any action or omission aimed at revealing the identity of an informant who has opted for anonymity is prohibited—even if the actual disclosure does not occur.

4.2 SUPPORT MEASURES FROM OBLIGED ENTITIES

The first measure of support (Art. 20 of the Directive) is offering comprehensive and independent information and advice that is easily accessible to the public and free of charge. This includes guidance on: a) procedures and remedies available, b) protection against retaliation, and c) the rights of the person concerned. Additionally, whistleblowers should receive effective assistance from competent authorities before any relevant authority involved in their protection against retaliation. This includes:

A. certification, where provided for under national law, confirming that they qualify for protection;
B. legal aid in criminal and cross-border civil proceedings, in accordance with Directive and Directive 2008/52/EC of the European Parliament and the Council (48);
C. where permitted by national law, additional legal aid, legal counselling, or other legal assistance in further proceedings.

4.2.1 The role of Authorities

A. the **competent authorities** must actively **support whistleblowers** who experience retaliation, serving as their first point of contact;
B. whistleblowers should report their situation to these authorities, which are **responsible for enforcing the Directive** within their Member State;
C. authorities assess whether the individual **meets the criteria for protection** and whether they have faced retaliatory measures;
D. authorities must ensure that whistleblowers receive proper legal recognition and assistance.

4.2.2 Forms of support provided by the Directive 2019/1937/EU

Recital 90 of the Directive provides that **competent authorities** should provide whistleblowers with the **support necessary** to effectively access protection. In particular, they should: a) provide **proof or other documentation** confirming to other authorities or courts that **external reporting** has taken place, and b) ensure whistleblowers understand **their rights and available resources.**

Seeking **professional guidance** can provide the confidence needed to navigate the process while ensuring the highest level of protection under the law.

Legal Action Against Retaliation

Free and **independent legal assistance** should be available to help whistleblowers navigate reporting processes and understand their rights. Some jurisdictions extend legal aid to **both civil and criminal proceedings** involving whistleblower protection cases. If a whistleblower **faces retaliation**—such as dismissal, demotion, or harassment – they have the right to **seek legal remedies**, including interim relief and full compensation (art. 21.8).

To support their claim, whistleblowers **must provide evidence** showing that they made a report and that retaliatory actions were taken against them. **National courts and tribunals** play a crucial role in **enforcing these protection**s, ensuring that affected individuals are restored to their previous status and compensated for any harm suffered.

In court[58] proceedings concerning damage suffered by a whistleblower, if the whistleblower demonstrates that they have reported a violation and

[58] Art. 38.4 Spanish law 2/23, Bulgarian... art. 19 Italian law 24/2023

suffered harm, it is presumed that the damage resulted from retaliation. In such cases, the burden of proof shifts to the party that took the adverse measure, they must demonstrate that the action was based on duly justified grounds.

A practical example in Spain: a fund was established for free legal, social and psychological support for whistleblowers. The **Netherlands** has implemented a similar initiative. In **France**, whistleblowers can receive provisions for legal costs and subsidies in appeals against retaliatory measures or in defending themselves against legal action aimed at hindering their reporting or public disclosure.

It is interesting to note that in **Italy,** in cases of attempted or threatened retaliation, the implementing law provides that the whistleblower must present elements showing the likelihood (*"fumus")* of the threat or attempted retaliation. The burden of proof then shifts to the party accused of retaliation, requiring them to demonstrate that the alleged acts are unrelated to the whistleblower's report. This is the reverse of the burden of proof provided by the Directive as mandatory. In Italy it is provided by the implementing law, not required by ANAC.

In addition to legal aid, whistleblowers **may receive psychological and financial support**, especially when retaliation causes emotional distress and/or economic hardship. In some cases, authorities may formally recognize a whistleblower's status, reinforcing their legal protection and credibility.

Accessing Support Services

To further safeguard whistleblowers, Member States are required to establish independent advisory services that provide legal aid, practical guidance, information, and support. Whistleblowers can turn to these services for confidential advice regarding their rights, available remedies, and legal options. These support structures are designed to empower individuals, ensuring they can navigate the reporting and protection process with confidence. According to the Directive, these services may be provided either by a public institution or by civic entities.

Spanish law explicitly allows for effective assistance from any relevant authority involved in protecting whistleblowers from retaliation, including the issuance of certification confirming their eligibility for protection under the law.

Retaliation Beyond the Workplace

Retaliation against whistleblowers extends beyond workplace consequences such as dismissal or demotion. It can also include:

A. harassment and intimidation;
B. reputational damage;
C. social media smear campaigns;
D. industry blacklistings, which can severely impact a whistleblower's career prospects.

The Directive explicitly addresses these risks, ensuring protection beyond the workplace and acknowledging that whistleblowers may face wider societal consequences.

Italian law explicitly ensures a protection covering also the retaliations that may consist of economic or financial harm, including loss of economic opportunities and loss of income; early ending or cancellation of the contract for the supply of goods or services; cancellation of a license or permit; unjustified request for psychiatric or medical examinations.

Certification by Competent Authorities

In certain Member States, formal whistleblower status is a prerequisite for receiving support and protective measures. In some Member States, the status of whistleblower is recognized upon the provision of a “whistleblower certification” as outlined in Recital 90(1) of Directive.Among the countries that have introduced this certification are France, Latvia, Poland, and Spain, specifically in the case of Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community Region (AVAF). This certification serves as formal recognition of their status and can be useful in legal proceedings or when seeking assistance from public or private institutions. It strengthens their case when they need to prove their entitlement to protective measures.

Under **certain national frameworks, whistleblowers may qualify for certification**, confirming that they meet the legal requirements for protection. However, even in the absence of certification, whistleblowers should have effective access to **judicial review**. Courts will ultimately decide—based on all the individual circumstances of the case, whether a whistleblower qualifies for protection under the applicable rules.

4.3 EXPANDING THE SCOPE OF BREACHES

While the Directive primarily focuses on EU law violations, it encourages Member States to extend protections to breaches of national law and unethical conduct that, while not illegal, poses risks to society. By broadening the scope of protected disclosures, Member States can strengthen whistleblower safeguards, ensuring greater protection against misconduct that may harm public interest, democracy, or institutional integrity.

GENDER BOX

Protecting whistleblowers requires an **inclusive approach**, recognizing that individuals from **marginalized groups** or those facing intersectional vulnerabilities may experience **higher risk of retaliation** and greater fear than others. The risk of retaliation **can influence** whether and how a person decides to blow the whistle. Research, including studies conducted by Transparency International, confirm that women may experience greater fear and stress when reporting misconduct (see Gender Box in Chapter 5).

Ch. 5 >

One of the main factors influencing women's decision to report misconduct is the power dynamics within the workplace:

A. power imbalances within the organisation: Work environments are often dominated by men in positions of power and decision-making authority. The greater the **power imbalance** between men and women, the higher the risk of retaliation for female whistleblowers;

B. retaliation against women often targets their personal sphere: Unlike other forms of retaliation, women may experience **intimate and personal attacks**, such as sexist comments or gender-based harassment;

   I. Bulgaria: Civil society organisations have raised concerns over the increasing number of legal actions against female whistleblowers in journalism. Female journalists are often perceived as the weaker sex, making them easier targets for intimidation and fear tactics;

C. health and psychological impact: Research shows that women take **sick leave** more frequently than men after reporting misconduct, often as a way to avoid retaliation in the workplace;

D. Italy: Studies have highlighted that the disadvantages faced by women in whistleblowing also manifest as **lower awareness** of their rights and reduced ability to protect themselves in legal proceedings.

To address these gender-based challenges, organisations should:

A. **develop and approve gender-sensitive protocols (See Box in Chapter 1):**

   I. with consensus and adequate representation, organisations should establish specific protocols or guidelines for handling gender-related whistleblowing cases;

   II. ensure these protocols are integrated into both whistleblower protection policies and the organisation's equality and non-discrimination policies.

   III. these protocols should outline clear procedures for reporting, investigating, and addressing cases of gender-based violence, harassment, or discrimination;

   IV. all individuals should be fully informed of their rights and the support services available.

B. **expand access to legal aid, psychological support as well as external services:**

   I. ensure legal aid is widely available to women and other groups exposed to discrimination, so they can better defend themselves against retaliation and legal actions;

   II. ensure that reporting mechanisms are designed to prevent retaliation and re-victimisation in gender-based cases, making sure reports cannot be accessed by individuals within the same workplace hierarchy, such as supervisors or colleagues. Whistleblowers need to feel safe that their identity and actions will be protected, especially in sensitive gender-based cases where the risk of retaliation is higher;

   III. provide information on external support services, including legal aid, psychological support, and survivor advocacy organisations. This allows potential whistleblowers to feel more secure and informed when considering whether to report misconduct and to face any challenges they may face during the process.

Ch. 1 >

Specifically, in Spain the material scope **of protection applies to individuals who report both actions or omissions provided for in the material scope** of the Directive, as well as, actions or omissions that may constitute a serious or very serious criminal or administrative offense in the Spanish legal system, and "in any case, all those serious or very serious criminal or administrative offenses that involve economic loss for the Public Treasury and for the Social Security will be understood to be included" (Art. 2.1.b) Law 2/23).

4.4 PUBLIC DISCLOSURE AND EMERGENCY SITUATIONS

Whistleblowers are generally encouraged to report internally or externally before making their disclosure public. However, they remain protected if public disclosure (pursuant art. 15 of the Directive) is necessary due to imminent threats—such as environmental disasters, health risks, or financial fraud—or if evidence may be destroyed, or authorities are compromised[59]. (detail better: In Spain, whistleblowers must meet **specific requirements** to obtain protection when making a **public disclosure**. These requirements should be detailed, rather than relying on generic information. (*Consider adding the specific legal criteria required in Spain for public disclosures to be protected*.) In Italy too.

4.5 LOSS OF PROTECTION

Protection may be revoked under specific conditions to prevent misuse while maintaining integrity of the system:

A. **malicious reports**: Whistleblowers who knowingly provide false or misleading information lose their protection. Member States may impose penalties for such cases;
B. **failure to follow procedures**: Reporting outside designated channels typically results in the loss of protection, except in cases of urgent threats or evidence destruction;
C. **illegal activities**: Whistleblowers engaged in hacking, data theft, or unauthorised access are not protected to ensure responsible use of the system;
D. **breach of confidentiality**: If the whistleblower discloses excessive or sensitive information without justification, protection may be revoked;
E. **improper public disclosure**: Whistleblowers must first attempt internal or external reporting, unless there is a valid justification for urgent public exposure.

---

[59] According to the Spanish legislation a person who makes a public disclosure shall be eligible for protection under the Law "if the conditions for protection regulated in Title VII and any of the following conditions are met:

(a) That they have made the communication first through internal and external channels, or directly through external channels, in accordance with Titles II and III, without appropriate action having been taken thereon within the prescribed time limit.

b) That it has reasonable grounds to believe that either the breach may constitute an imminent or manifest danger to the public interest, in particular where there is an emergency situation, or there is a risk of irreversible damage, including a danger to the physical integrity of a person; or, in case of communication through an external information channel, there is a risk of retaliation or there is little likelihood that the information will be dealt with effectively due to the particular circumstances of the case, such as concealment or destruction of evidence, collusion of an authority with the perpetrator of the infringement, or that the authority is involved in the infringement.

2. The conditions for protection provided for in the preceding paragraph shall not apply when the person has disclosed information directly to the press in accordance with the exercise of the freedom of expression and truthful information provided for in the Constitution and its implementing legislation." (Art. 28, Law 2/23).

4.6 WHISTLEBLOWER SUPPORT: WHO CAN ASSIST?

The Directive (recital 41 and then art. 4) extends protections to those assisting whistleblowers, ensuring all involved can operate safely and effectively.

Facilitators

Facilitators, such as legal advisors and union representatives, help whistleblowers report breaches securely. Their role includes:

A. providing legal guidance;
B. ensuring compliance with reporting procedures;
C. maintaining whistleblower anonymity.

Art. 2.1 of the **Italian** law defines the facilitator as "the person who assists the whistleblower in the reporting process, working in the same context and whose assistance must be confidential". The assistance offered by the facilitator may consist of advice or support to the reporting person. For example, the facilitator could be a colleague of the reporting person who assists the latter in a confidential way.

Art. 5 of the **Bulgarian** law stipulates that protection shall also be granted to "persons who assist the whistleblower in the whistleblowing process and whose assistance shall be confidential". The law does not refer to these persons as "facilitators" and does not provide any details on what this assistance may consist of.

Spanish law expressly recognizes facilitators as protected subjects. According to Article 3.3 of the Law: Also covered by this Law are the natural persons who assist the whistleblower in the process, including those who provide support in the work environment, and those who are related to him and may suffer retaliation in a labor or professional context, as well as legal persons owned by the whistleblower, for whom he works or with whom he maintains a relationship in a labor context or in which he holds a significant participation.. This includes facilitators such as legal advisors, union representatives, co-workers and persons providing psychological or institutional support.

Their protection is intended to prevent indirect retaliation and to ensure that the whistleblower can act safely, especially in sensitive work environments. This extension of the subjective scope of protection responds to the provisions of Recital 41 and Article 4 of the Directive, ensuring that all persons involved in good faith in the whistleblowing process can operate without fear of negative consequences.

Third-Party Organisations

NGOs and civil society groups can:

A. offer support to potential whistleblowers acting as information centers (see below), by providing practical advice on reporting and legal rights, assistance with reporting, psychological support to help whistleblowers manage stress and societal backlash;
B. offer safe channels and visibility for public disclosure, facilitating access to the media or enabling publication through independent platforms.

Competent Authorities

State-designated authorities:

A. guide whistleblowers on reporting procedures;
B. explain protection mechanisms;
C. certify whistleblower status where applicable, to prevent retaliation.

Information Centers

Independent administrative bodies serve as centralized hubs for whistleblower support, offering legal advice, counseling, and coordination of available resources. Also civil Society Organisations can cover this role. In Italy, the law assigns a crucial role to Third Sector organisations in supporting whistleblowers. The organisations provide information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legislation, on the rights of the accused person, and on the terms and conditions of access to legal aid.

Supportive Colleagues and Supervisors

Trusted colleagues or supervisors can:

A. provide informal support;
B. help refine reports to ensure accuracy;
C. assist in using internal reporting channels correctly.

Legal Aid Providers

Both public and private legal aid organisations assist whistleblowers who face retaliation, supporting them in legal proceedings to seek redress or defend their rights.

Psychological and Social Support

Potential whistleblowers who are not sure about how to report or whether they will be protected in the end may be discouraged from reporting, the Directive (cons. 89 and art. 20) provides that Member States are encouraged to provide counseling and social support services tailored to help individuals cope with the emotional and social challenges they may face. This is part of

the protection measures and includes offering access to psychological counseling, as well as legal and financial advisory services to mitigate potential professional and economic repercussions. Additionally, support networks, such as peer groups or mentorship programmes, can help whistleblowers navigate societal backlash and reduce feelings of isolation. Public awareness campaigns can also play a role in fostering a culture that values whistleblowing, reducing stigma, and encouraging solidarity within communities and workplaces. By implementing these measures, Member States can create a more supportive environment that not only protects whistleblowers but also empowers them to act in the public interest without fear of retaliation.

Financial support

Only some countries offer economic support measures in their legal framework, but it is limited in the scope and in the amount. Among them, Belgium and Slovakia cover costs of private legal aid and costs of private health and/or psychological expenses.

Protections for Assistants

The Directive also protects those who assist whistleblowers, including:

A. facilitators;
B. family members;
C. colleagues.

This ensures they can help whistleblowers without fear of retaliation.

Press Freedom and Access to Information

A free press plays a critical role in ensuring whistleblowers can safely share disclosures. Governments must protect media independence, safeguard journalists covering whistleblower cases, and uphold source confidentiality. Additionally, access to information is crucial: whistleblowers need transparent legal frameworks that allow them to substantiate their claims with evidence.

OPEN GOVERNMENT BOX

Whistleblower protection

An effective protection for whistleblowers would benefit from coordinated efforts among diverse actors such as institutions, media organisations, civil society groups, trade unions, and human rights bodies. This collaborative approach recognises the crucial role of whistleblowers across sectors and strengthens the narrative linking their reporting and protection with labour rights and freedom of expression. This connection is particularly relevant in countries experiencing a rise in strategic lawsuits against public participation (SLAPPs).

Practitioners across sectors have indicated that when the Directive is implemented through the creation of new dedicated authorities or offices responsible for whistleblowing, **multi-stakeholder engagement can be decisive in building trust among all parties involved**, especially if carried out within the framework of the country's OGP implementation. Processes like those found in the Open Government Partnership (OGP) offer a useful platform for such multi-stakeholder dialogue. In particular, this can help to further deepen participation of private sector representatives - whether as individual entities or through representative bodies - and thus contribute to a more balanced discussion and more effective protection mechanisms.

Meaningful stakeholder engagement should also **extend to participation in international fora such as the United Nations Convention against Corruption (UNCAC).** This includes ensuring that whistleblowers themselves, as well as organisations dedicated to their protection, are actively involved in national delegations and preparatory discussions. A strong example of this approach was seen at CoSP10 to the UNCAC in Atlanta[60], where the resolution on the protection of reporting persons was spearheaded by a former whistleblower who was directly included in the Serbian delegation. This demonstrates the value of incorporating firs-thand experience into policy-making, ensuring that those who have faced retaliation or navigated the reporting process contribute to shaping more effective protections. **By integrating whistleblowers and advocacy groups into official delegations, working groups, and negotiation processes**, countries can develop policies that are not only well-informed but also practical and enforceable. This inclusive approach enhances legitimacy, strengthens international cooperation, and ensures that whistleblower protection frameworks are rooted in real-world challenges and needs.

In addition to these collaborative measures, CSOs strongly recommend a **broad interpretation** of whistleblower protection laws, going beyond the provisions of the Directive and paving the way for its future reform.

A. one key proposal is to extend safeguards to **organisations that provide support and advice to whistleblowers**, ensuring that those who assist reporting persons are also shielded from threats and retaliation. Governments and civil society can collaborate on this expansion, recognising the crucial role these organisations play in enabling safe and effective disclosures;

B. another crucial step is achieving **greater harmonisation** between whistleblower protection mechanisms and other legal frameworks, such as those designed for **witness protection programmes and reporting as it relates to corruption involving organised criminal groups.** A more integrated approach would help ensure that individuals who expose wrongdoing receive adequate security measures;

C. despite not being explicitly covered by the Directive, CSOs advocate for extending protection to cases where misconduct or corruption is exposed **through access to public information**. This includes disclosures made by **journalists, NGOs, legal advocates, and active citizens** who, in the public interest, uncover and report irregularities.

[60] In this regard see: https://whistleblowingnetwork.org/News-Events/News/News-Archive/Governments-Around-the-World-Step-Up-to-Support-Wh

Several international instruments support this broader interpretation of whistleblower protection. The EU Whistleblower Directive 2019/1937/EU itself, the European Media Freedom Act (EMFA), and the UN Convention Against Corruption (UNCAC) with related resolutions, all contribute to creating a more favorable legal environment for expanding and harmonising safeguards. By strengthening legal protections and expanding their scope, governments can enhance transparency, encourage accountability, and create safer conditions for those who speak out against wrongdoing in both public and private sectors.

Whistleblower support

A positive Open Government initiative in support of potential whistleblowers is to establish a **public registry of CSOs who provide free support and advice services**, to enhance their recognition and visibility. In Italy's case, this objective was achieved by including the commitment in its 5th National Action Plan (5NAP) for Open Government (2021-2023)[61]. For those who wish to replicate the Italian initiative, we recommend to:

A. define the requirements for CSOs to enter the public list, to ensure impartiality, respect for privacy regulations and competence;
B. foster diverse professional expertise within CSOs to ensure holistic support (legal, psychological, ...);
C. provide for a formal convention with the authority for suitable CSOs;
D. maintain an active working group among the members of the register to monitor training and information needs and facilitate peer exchange;
E. establish at least biannual forums to address systemic challenges faced by CSOs and concerns arising from real cases, while respecting the protection of confidentiality;
F. encourage or require all public bodies to follow the example of the authority in making the list visible also on their website and in communication to their employees;
G. a further advanced measure within an Open Government framework is establishing coordination and networking among recognised advisory and support entities to ensure that potential whistleblowers are directed to the most suitable organisation for guidance. For example, a **centralised hub** could be created to collect and assess whistleblowers' needs, then refer them to the appropriate support organisation based on territorial or sector-specific expertise. This would help streamline the process and ensure individuals receive the most effective assistance.

Such legal and psychological support services should be free for potential whistleblowers, to remove any economic barriers to accessing services. To ensure this, the government should secure **public funding to support organisations** (institutional and civic ones) and **free legal aid** for whistleblowers if it comes to trials.

[61] In this regard see: https://www.opengovpartnership.org/members/italy/

FINAL RECOMMENDATIONS

To offer comprehensive support and protection to individuals accessing reporting procedures, it is of paramount importance to foster an effective and collaborative approach to whistleblowing. This requires the involvement of multiple stakeholders, each contributing their expertise and role in addressing the challenges associated with whistleblowing. Key measures to enhance whistleblower support and protection include:

1. IMPROVING ACCESS TO WHISTLEBLOWER SUPPORT

Public and private entities should improve accessibility by publishing lists of civil society organisations (CSOs) and other relevant bodies that offer assistance and information to whistleblowers;

2. PROMOTING CONTINUOUS COOPERATION

Continuous cooperation between competent authorities, CSOs, and other relevant organisations is crucial to ensuring they are well-equipped to provide high-quality services to whistleblowers;

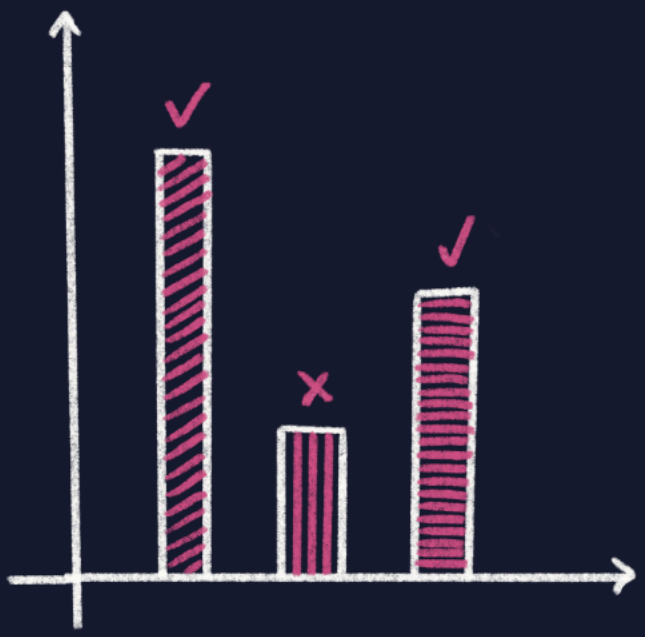
3. ENHANCING AWARENESS AND TRAINING INITIATIVES

Administrations and companies must actively promote awareness-raising initiatives and training programmes to enhance understanding of whistleblowing regulations and procedures. In addition, targeted training courses for public officials should be implemented to develop best practices for handling whistleblowing reports and effectively managing related processes;

4. FACILITATING DIALOGUE THROUGH DEDICATED MEETINGS

Lastly, organizing dedicated meetings with representatives from both the public and private sectors can facilitate constructive dialogue, allowing stakeholders to address common challenges and identify optimal solutions collaboratively.

Measurement and evaluation of system effectiveness and assessment of the whistleblowing culture



Chapter 5

Open the whistle

MEASUREMENT AND EVALUATION OF THE EFFECTIVENESS OF THE SYSTEM AND ASSESSMENT OF A WHISTLEBLOWING CULTURE

Chapter 5

5.1 MEASURING WHAT MATTERS: EFFECTIVENESS, AWARENESS, AND CULTURAL FIT

Effective whistleblowing systems contribute to **strengthening transparency** and **accountability** in the EU. To ensure their impact, the effectiveness of these systems, along with the level of awareness and understanding of the whistleblowing process, should be regularly measured and evaluated. With the Directive, despite challenges such as delayed transposition in most Member States, incomplete integration into national legal systems, and the framework's apparent complexity, attention has shifted toward evaluating the effectiveness of these systems and the cultural factors that influence their success.

In Bulgaria it has been highlighted that there is some confusion and that employees sometimes struggle to understand the scope of the Directive, particularly when it comes to employment rights or violations that may seem personal rather than affecting the wider public interest. **An Italian respondent** acknowledged that the new whistleblowing legislation has introduced positive innovations, but highlighted a number of critical issues, such as a coordination problem in the case of disclosures through social media.

In **Spain,** it has been highlighted that the implementation of the law should have been accompanied by procedural reforms, including the strengthening of protection measures.

Recent developments highlight the need to evaluate whistleblowing systems not merely as compliance tools, but as **integral mechanisms** for promoting ethical behaviour and organisational integrity. Contemporary research and practice highlight the need for comprehensive evaluation methods to ensure whistleblowing channels are accessible, trustworthy and effective in addressing wrongdoing while protecting whistleblowers from retaliation. Moreover, the cultural dimension – encompassing trust, awareness and employees' willingness to report – has emerged as a cornerstone in creating a **proactive speak-up culture.**

5.2 REVIEW OF EXISTING MEASUREMENT AND EVALUATION TOOLS

5.2.1 International Organisation for Standardization

The ISO 37002:2021 framework serves as an analytical tool for policy-making and offers insights into the implementation of Whistleblowing Management Systems (WMS) across different institutions.[62] It provides guidelines for establishing, implementing and maintaining an effective WMS based on the principles of trust, impartiality and protection. The framework outlines four key steps:

A. receiving reports of wrongdoing;
B. assessing the reports received;
C. considering the received reports, and;
D. closing whistleblowing cases. Designed to be universally applicable, these guidelines are relevant for organisations of all sizes, types, and sectors including public, private and not-for-profit entities.

The framework provides a standardised approach to evaluating whistleblowing systems, aiming to facilitate policy-making and governance improvements. Existing case studies highlight that the implementation of this standard for whistleblowing management systems is often partial and requires further development in specific areas, such as whistleblower awareness and protection policies. Consequently, the framework may need to be adapted to meet specific organisational needs.

5.2.2 Digital reporting platforms

The Digital Services Act (DSA)[63] introduces tools to create a safer, fairer, and more transparent online space in the EU.[64] Among these is the DSA whistleblower tool, which allows to identify harmful practices of very large online platforms and online search engines (VLOPs/VLOSEs).[65] It provides a secure, and optionally anonymous, channel for reporting internal information (such as reports, notes, email exchanges, data metrics, internal research, decisions and other relevant circumstances, whether past, present or future) to the Commission. However, the scope of reporting is limited to practices breaching DSA obligations such as content moderation, functioning of recommended systems, advertising, assessment and mitigation of risks related to users' fundamental rights, public safety and health concerns, civil discourse, electoral processes, and children's rights. While digital platforms improve the accessibility and efficiency of reporting, their limitation lies in offering reporting on a narrow range of issues. Moreover, their use and effectiveness depends heavily on user acceptance and trust in the system.

---

[62] In this regard see: International Organisation for Standardization, ISO 37002:2021. Whistleblowing management systems — Guidelines, https://www.iso.org/obp/ui/en/#iso:std:65035:en

[63] In this regard see: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

[64] In this regard see: European Commission. Digital Services Act whistleblower tool: Report inside information about online platforms, https://digital-services-act-whistleblower.integrityline.app

[65] In this regard see: European Commission. Supervision of the designated very large online platforms and search engines under DSA, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-lqfbha7w

5.2.3 Empirical surveys: Polish and Italian experiences

An empirical survey was conducted in December 2022 among HR professionals, managers, and directors in Poland, prior to the Polish Whistleblower Act coming into force on 25 September 2024. The survey focused on whistleblowing within the broader context of personnel risk, examining managers' attitudes toward risk, sources of personnel risk, the effectiveness of HR compliance systems (including whistleblowing mechanisms), and behaviours and losses related to human-factor risks. Data collection employed both Computer-Assisted Web Interviewing (CAWI) and Computer-Assisted Telephone Interviewing (CATI) methods. Statistical analyses, including the chi-square test with Yates' correction and the Kruskal-Wallis test, were applied to assess differences in evaluations of whistleblowing processes based on variables such as job position, company size, ownership form, and industry sector.[66]

Key results from the **Polish** survey are:

A. whistleblowing is widely regarded as an important tool both for detecting wrongdoing in organisations and for effective compliance management;[67]
B. one-third of respondents lacked a clear opinion on the effectiveness of well-established whistleblowing systems;
C. in medium-sized companies, respondents provided higher ratings for internal whistleblowing channels and protections against retaliation compared to other organisations. The differences in scores based on job position can be attributed to variations in organisational culture, employee confidence in the effectiveness of whistleblowing systems, the scope of reportable wrongdoing, and the adequacy of internal channels.

On average, professionals rated their organisations' whistleblowing systems lower than the rest. HR professionals, managers and HR directors disagreed in their assessment of the existing level of employee confidence in the proper functioning and reliability of their companies' whistleblowing systems.[68]

A parallel empirical study was conducted in **Italy** by the National School of Administration (SNA) within the framework of the project "Training for Change. Open Administration and Innovative Training Models for the Efficient Implementation of Whistleblowing"[69]. The aim was to assess the impact of SNA training programmes on the perception of whistleblowing, given its relatively weak entrenchment in Italian legal and organisational culture.

The Italian study employed a methodology similar to the Polish survey, using both CAWI and CATI techniques. Data were collected from a sample of HR professionals, managers, and public officials, applying statistical analyses

---

[66] Winnicka-Wejs, A. "Whistleblowing as a tool for HR compliance management system – survey report". Scientific Papers of Silesian University of Technology 2023. Organisation and Management Series no. 182, 2023, pp. 573-596. DOI: 10.29119/1641-3466.2023.182.34. https://managementpapers.polsl.pl/wp-content/uploads/2023/12/182-Winnicka-Wejs.pdf

[67] Ibid.

[68] Ibid.

[69] Donini, V. M., Lostorto, V., & Zamaro, N. (2022). Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente, 4(2022). https://www.amministrativamente.com/index.php/formez/article/view/13339

such as the chi-square test with Yates' correction and the Kruskal-Wallis test to examine differences based on job position, organisational structure, and sector.

Key results from the **Italian** survey are:

A. training plays a crucial role not only in disseminating awareness and knowledge about whistleblowing, but also in transforming public perception of it;
B. trust and cultural barriers remain major challenges despite legal protections;
C. support role of Civil Society Organizations is underused and not well known (prior to the training only 13% of respondents were aware of their role, after training the percentage rose to 46,6%);
D. internal channels are less preferred (38% of respondents) and many favor external reporting (61%) because it is considered more reliable, independent and effective;
E. the primary incentives for reporting wrongdoing are: protection from retaliation (74,2% women, 67,9% men), confidentiality assurances (68,5% women, 67% men), knowing that the reported activity will be addressed (59,2% women, 57,8% men), and knowing that the issue I raised is considered important/serious (41,7% women, 46,4% men);
F. a monetary reward is not regarded as a meaningful incentive (only 3,8% women, 7,3% men);
G. the study underscored the need for further training to increase awareness, promote whistleblowing as an ethical duty, and enhance protections to build trust in the system.

Besides, always with reference to **Italy**, it is interesting to notice that ANAC, the National Anti-Corruption Authority, submitted a questionnaire to public and private sector entities aimed at verifying the solutions adopted in a phase of initial application of the legislation. In the public sector, 62% of the entities have set up an IT platform specifically dedicated to the acquisition and management of reports in written form. 38% have not set up a platform and have adopted different methods of receiving reports, such as certified email or ordinary mail.

Two critical aspects are highlighted in this regard:

A. among the entities that have not adopted the platform there are also big administrations, which would have all the tools, in terms of availability of human and material resources, to more easily establish the IT infrastructure;
B. certified electronic mail and ordinary mail do not constitute adequate methods of receiving reports, if not assisted by specific countermeasures aimed at mitigating the risk of improper disclosure of data.

The same critical profiles highlighted above were also found in the private sector: only 56% of the subjects, in fact, activated the IT platform and approximately 64% declared that they had foreseen the possibility of making oral reports. Furthermore, it is interesting to note that, in the private sector, only 30% of the entities declared that they had received whistleblowing reports: this is a sign that the whistleblowing framework is still little known and must be further encouraged.

Both the Polish and Italian studies reveal that, despite recognising the importance of whistleblowing, employees often lack confidence in the effectiveness of reporting mechanisms and fear retaliation. While training initiatives, as seen in the Italian study, help to improve awareness, cultural barriers and institutional weaknesses continue to hinder the establishment of robust whistleblowing cultures. Addressing these challenges requires not only legal frameworks but also proactive organisational policies, clearer communication, and strengthened protections to foster a culture of integrity and transparency. While the survey results are not representative and cannot be generalised nationally, they may be useful for business owners, managers, HR professionals, and compliance officers, who are all key stakeholders responsible for implementing effective whistleblowing systems in the workplace.

5.2 INDEX FOR EVALUATION OF WHISTLEBLOWER PROTECTION (IEWP)

Some researchers have developed an **Index for Evaluating Whistleblower Protection (IEWP)**, a digital tool to assess the **effectiveness of protection mechanisms** across different countries and time periods.

The IEWP consists of both quantitative and qualitative sub-indices. **The first evaluates** institutional safeguards through indicators, such as job security, confidentiality, protection from retaliation, legal immunity, whistleblower protection rates (number of protection requests compared to corruption reports, etc.). **The second focuses on capturing** perceptions and experiences related to whistleblowing, including the perceptions of various groups (officials, experts, citizens with no whistleblowing experience, and whistleblowers themselves) and experiences (only of whistleblowers).

The IEWP enables comparisons of whistleblower protection levels across countries and tracks changes over time. Beyond measurement, it highlights key improvement areas, such as timely implementation of laws, impartiality in appointing officials, and **transparency in data availability**.

The authors advocate for a two-pillar methodology, combining administrative data with survey responses, and emphasize the need to standardize and improve access to relevant data.

5.2.1 Transparency International

Following the publication of a methodology for assessing the compliance of draft legislation with the EU Whistleblower Directive and best practice,[70] Transparency International has developed a self-assessment framework to help organisations set up, implement and review internal whistleblowing systems (IWS) that are effective and in line with best practice and international standards.[71] The framework includes 130 questions covering eight dimensions ranging from the system's scope and the protection it provides, to communication within and about the system, and monitoring

[70] In this regard see: Transparency International. Assessing Whistleblowing Legislation: Methodology and Guidelines for Assessment Against the EU Directive and Best Practice. 23 September 2020, https://www.transparency.org/en/publications/assessing-whistleblowing-legislation

[71] In this regard see: Transparency International. Internal Whistleblowing System Self-assessment Framework, https://forms.office.com/Pages/ResponsePage.aspx?id=d2r57HSK7U-hwgM32S0wX1aBYjEGkw1JtPtUD4e4zF1UM0pCTTkwQVVKWFRIN1kyTzU3UFVRRE1MNy4u

its effectiveness.[72] The questions are designed to identify potential factors that could undermine the IWS. The answers and findings can help organisations improve the effectiveness of their IWS in line with best practice and international standards.

5.3 KEY INDICATORS FOR EVALUATING WHISTLEBLOWING SYSTEMS

Building on existing tools and means, and taking into account the state and needs of whistleblower protection systems within the EU and its Member States, this section aims to formulate a set of **quantitative and qualitative indicators** that can be used to assess the effectiveness of whistleblowing mechanisms.

On the quantitative side, key evaluation indicators relate mainly to the functioning of the reporting mechanisms. They should include, among others:

A. reports received and substantiated reports: the total number of whistleblowing reports received and the proportion of those substantiated following investigation over a specified period (e.g., annually);
B. inspections and their outcomes: the number of inspections carried out and their results;
C. response/resolution times: the average time taken to confirm, investigate, and resolve issues related to whistleblowing reports;
D. accessibility of reporting channels: the availability of gender-based, diverse, easy-to-use channels (e.g., online forms, hotlines, face-to-face options), their usability across different demographic groups, and respect for gender equality;
E. court proceedings and judgements: the number of court proceedings initiated, including proceedings to terminate retaliatory actions, and the judgments delivered over a specified period (e.g., annually);
F. Incidents of retaliation and protective measures: the number of whistleblowers who have experienced retaliation and the measures taken to address such cases (effectiveness of protection);
G. anonymity and confidentiality: the existence of measures to protect whistleblowers and ensure anonymity;
H. follow-up actions: the share (percentage) of cases that result in corrective actions or policy changes;
I. financial penalties and recoveries: collected amounts collected from fines and other imposed financial sanctions imposed;
J. assessment of financial damage: evaluation of financial losses linked to reported misconduct.

[72] In this regard see: Transparency International. Internal whistleblowing systems: self-assessment framework for public and private organisations, 31 October, 2024, https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations

The identified indicators provide measurable information on the performance of the system. Data collection methods for these indicators may include:

A. surveys and questionnaires distributed to employees and stakeholders to measure awareness, trust, and perception of the reporting systems;
B. analysis of report statistics, resolution rates, and protection outcomes, court statistics, and related metrics (data analysis);
C. assessment of compliance with whistleblowing legislation and guidelines, internal rules, and policies (compliance audits).

In countries, such as **Bulgaria**, where measuring the effectiveness of the whistleblowing system is difficult due to the low number of reports and court cases, the focus should shift towards building trust through positive experiences and transparency. Swift action following a report and ensuring confidentiality are key to building confidence in the system and encouraging more employees to use it. If employees see that reports lead to real results and that whistleblowers' identity is kept confidential, they would be more motivated to participate.

As regards qualitative feedback, the focus should be on indirect or anonymous approaches, such as aggregated surveys, desk research, or secure feedback channels that ensure the confidentiality and protection of whistleblowers. These include:

A. focus groups conducted separately with employees and whistleblowers to explore experiences with the system and cultural attitudes toward reporting;
B. case studies:
   I. analysis of the whistleblower protection framework, including compliance with EU Directive, national legislation, internal rules and procedures (legal compliance), as well as the availability of psychological support, legal aid, and other measures for whistleblowers (support mechanisms);
   II. analysis of specific whistleblower reports to evaluate process handling and outcomes;
   III. analysis of financial proceeds of fines and penalties, and assessment of identified financial damages.
C. stakeholder interviews with external actors, such as civil society organisations, professional associations, trade unions, and regulators, to explore collaboration and systemic impact.

To encourage whistleblowing and improve the whistleblowing systems, additional tools can be recommended, such as:

A. publishing detailed assessments of the whistleblowing systems' performance and the culture of whistleblowing;
B. collecting regular feedback from whistleblowers, employees, and stakeholders to identify gaps;
C. using evaluation results to refine reporting mechanisms, training programmes and protection frameworks.

5.4 ASSESSING THE SPEAK-UP CULTURE

A robust speak-up culture is essential for the success of whistleblowing systems.

In this sense, methods to assess employees' confidence in reporting channels, their willingness to report violations, and their perception of management's responsiveness are important. At various EU levels confidentiality, including the protection of whistleblowers' identity, is recognised as a fundamental and effective way of encouraging employees to report problems.[73]

A range of tools assessing employees' awareness, their trust in the whistleblowing protection system, the frequency of reporting, etc., can be used to assess engagement in speak-up culture:

A. the proportion of employees who are aware of reporting mechanisms and of their rights as whistleblowers can be used to assess employee awareness;
B. surveys to measure employee confidence in the organisation's response to whistleblower reports;
C. employees' reported willingness and ability to report.

Tools such as surveys and focus groups can also be used to identify barriers to speaking up, and to support strategies for creating an open and supportive environment for whistleblowers:

A. surveys or interviews with managers on their perceptions of whistleblowing and openness of reporting can provide information on management/leadership attitudes;
B. external stakeholders' confidence in the organisation's commitment to whistleblower protection is a measure of public trust;
C. feedback from whistleblowers on the fairness and transparency of investigations is an important indicator of the level of satisfaction with the resolution of whistleblowing issues.

To ensure widespread awareness, it is essential to:

Raising Public Awareness: for example, stakeholders from **Italy** reveal interesting insights on this topic. In order to spread a whistleblowing culture in society, the whistleblowing message needs to be conveyed through means that can reach a wider audience. To encourage a culture of whistleblowing, it is suggested that the Lega Serie A could use its large Sunday crowds to launch an awareness campaign and "act as a mouthpiece on such a sensitive issue, as it has done on other issues such as discrimination, abuse, femicide, etc.". Another suggestion is to develop key elements of communication to assess the public perception of whistleblowing, such as: speaking-up culture, community journalism, solution journalism, public service and collective issues. For others, the idea of whistleblowing should be seen as a democratic freedom, one of the manifestations of democracy that should be defended alongside freedom

[73] In this regard see: European Data Protection Supervisor (EDPS). Guidelines on processing personal information within a whistleblowing procedure, December 2019, https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whisteblowing_guidelines_en.pdf?utm_source=chatgpt.com

of expression. Furthermore, the definition of whistleblowing as a form of freedom of expression is seen as an important innovation in the legal framework for whistleblowing. An interesting approach is also proposed to counter the culture of silence and establish a new ethic – increasing the responsibility of citizens, spreading the awareness that reporting irregularities is a personal choice, reinforcing the understanding that the whistleblower is an ordinary person doing an ordinary thing. In addition, it was stressed that a culture should be created to make the system less and less institutional, for example by empowering citizens to take responsibility, as a culture of de-responsibility/irresponsibility could lead to a flood of slanderous or untrue reports made for personal gain, overwhelming the reporting systems.

The need to change the culture and the mindset that whistleblowers are not informants but collaborators, to see whistleblowers as an intelligent source of information and to show potential whistleblowers that reporting is not futile and that there is a need to build trust in the process was expressed by stakeholders in **Spain**.

From **Spain** arose a widespread culture of silence, driven by fear of retribution and exclusion from the group, which can be seen in the workplace in a similar way to children at school, where anyone who points out inappropriate behaviour is seen as a snitch.

In **Bulgaria** it has emerged that the culture of whistleblowing appears to be underdeveloped, and that staff have little interest or confidence in using the system. Interviewees shared the understanding that a confident whistleblowing culture needs to be underpinned by trust mechanisms with regular evaluation of the effectiveness of the system. Respondents argued that improving the confidence and effectiveness of the system would require continuous feedback, monitoring and adjustment of procedures. Suggestions included conducting regular reviews of internal policies and sharing experiences with other organisations to improve the overall whistleblowing culture.

According to practicing lawyers in **Bulgaria**, a clear link needs to be established, both legislative and in practice, as well as in public understanding, between the protection of freedom of speech in SLAPP (Strategic Lawsuits Against Public Participation) cases and the protection of whistleblowers. So far, this understanding is not visible in EU law, national law, legal practice, and public understanding. Legal practitioners are attempting to incorporate aspects of the SLAPP concept and the whistleblower protection legislation into the defence in defamation cases. While some jurisdictions have shown interest in this approach, the outcomes remain uncertain due to the absence of established case law. It is nevertheless expected that some of the outcomes of these cases will become clearer in the near future.

Exploring stakeholder perceptions and acceptance can provide important insights into the state of the speak-up culture, and help transform a culture of silence into a culture of active whistleblowing.

5.5 EVALUATING STAKEHOLDER ENGAGEMENT AND COLLABORATION

Stakeholders play a critical role in the success of whistleblowing initiatives, from supporting policies to acting on reported issues. It is therefore important to use appropriate methods to assess the effectiveness of stakeholders' collaboration, focusing on communication, alignment of whistleblowing policies and joint awareness-raising efforts. A set of indicators can be used to measure stakeholder collaboration.

Suggested indicators can measure:

A. frequency of engagement: number of joint training sessions, awareness-raising campaigns or forums with other stakeholders;
B. shared resources: existence and use of partnerships for shared resources (e.g., legal aid, investigation tools);
C. collaborative policy development: involving stakeholders in the development of whistleblower policies or guidelines;

A number of methods can be used to assess stakeholder engagement and collaboration in whistleblowing initiatives, including:

A. collaborative surveys to assess stakeholders' satisfaction with joint initiatives, providing insights into their perceptions of effectiveness and areas for improvement.
B. network analysis to map the flow of information and resources between stakeholders and identify strengths and gaps in communication and resource-sharing.
C. outcome analysis to measure the tangible impact of collaborative efforts, such as increases in whistleblowing reports or cases resolved.

OPEN GOVERNMENT BOX

Regular data collection and analysis of whistleblowing activities are key to assessing system efficiency. Indicators such as the ones mentioned in this chapter should ultimately inform policy adjustment. Open Government principles suggest that:

A. data is always published in **open data standards**;
B. data collection and transparency include information on **policy procedures and stakeholder engagement processes**;
C. findings are transparently communicated to and discussed with stakeholders, ensuring that **insights drive actionable improvements** that can be co-designed under a National Action Plan commitment or as a standalone Open Government Challenge, which allows for ambitious reform commitments to be made and recognized outside the regular Action Plan cycle.

In summary, to improve and make more transparent the regular assessments of the whistleblowing systems' effectiveness, the speak-up culture, and the engagement of stakeholders, the following minimum requirements are recommended:

A. regular publication, at least annually, of detailed assessments of the effectiveness of the whistleblowing system and the culture of whistleblowing;
B. regular collection of feedback from whistleblowers, employees and stakeholders to identify gaps and areas for improvement;
C. use of the evaluation results to refine reporting mechanisms, training programmes and protection frameworks.

In conclusion, while the legal framework of whistleblowing is in place at European and national levels, the necessary infrastructure and practical measures for its effective implementation is often lacking. The principle of Open Government requires the creation of an institutional mechanism, either a new institution or an existing one, to support the full, fair and responsible application of the whistleblowing legislation, help individuals in difficult situations, find reasonable solutions, and overall contribute to the improvement of both legislation and whistleblowing systems.

GENDER BOX

Regular data collection and analysis of whistleblowing activities are key to assessing system efficiency. Although women tend to condemn corrupt behaviour more than men, **they seem to report corruption less often than men**, as confirmed by Transparency International's Global Corruption Barometer (GCB) data[74].

Some **key findings** from different research:

A. only **48 percent of women believe they can report acts of corruption without the risk** of retaliation, compared to 54 % of men[75];
B. **incentives to report**: an experimental survey of over 2.000[76] employees showed how women are more incentivised than men to take action if there are **anti-retaliation protections and legal duty;**
C. according to study in Italy[77], there is no significant difference in the willingness to report between men and women. What needs to be further explored, however, is the **fear of retaliation from managers and colleagues**, and the **increased stress** women experience after reporting.

Overall, it seems that among the subjects interviewed for this toolkit, there is a tendency not to consider the difficulties and complexities of "**speaking out**" for women, but more generally for any marginalized group. However, if the data show that women tend to speak out less and suffer more from the fear of retaliation, this should serve as an indicator of the effectiveness of the system.

[74] 2021 Global Corruption Barometer by Transparency International

[75] 2021 Global Corruption Barometer by Transparency International

[76] In this regard see: rhttps://knowledgehub.transparency.org/assets/uploads/helpdesk/Gender-sensitivity-in-corruption-reporting-and-whistleblowing_2020_PR.pdf

[77] Donini, V. M., Lostorto, V., & Zamaro, N. (2022). Formare per trasformare: l'impatto trasformativo della formazione sulla prevenzione della corruzione. Prime riflessioni. Rivista di diritto amministrativo – Amministrativamente, 4(2022). https://www.amministrativamente.com/index.php/formez/article/view/13339

We recommend to:

A. **thematise the issue of women suffering more harm** and retaliation than men;

B. **raise awareness of an inclusive approach** to all diversities and weaker groups that may be present in an organisational culture;

C. raise awareness on cases of sextortion and sexual harassment. *To explore this topic further, see the box in **Chapter 1**;*

D. publication of data disaggregated **by gender** when available: only a small number of organisations include data on gender and intersectional factors. This gap represents a **missed opportunity** to gather up-to-date information that could support **evidence-based decision-making**. To address this issue, it is essential to **strengthen data collection** and analysis mechanisms, ensuring a more accurate understanding of whistleblowers' behaviour, needs, and priorities;

E. **training and Sensitization on Gender-Sensitive Whistleblowing**;

F. **develop a training programme within the organisation as a preventive measure**, aimed at educating all members and participants in whistleblowing practices, with a focus on gender and the intersection of other vulnerability factors, such as poverty and power imbalances. The programme should address the reporting of harassment, sexual abuse, and corruption-related misconduct, while highlighting the differing impacts on women and men, particularly the disproportionate burden on women. Emphasis should also be placed on preventing retaliation, such as sexual harassment or sextortion, and raising awareness about gender stereotypes, biases, and the specific vulnerabilities that impact whistleblowers in marginalized situations;

G. **define a MEL (Monitoring, Evaluation and Learning) of Gender-Sensitive Whistleblowing Practices:**

   I. implement regular audits to ensure that reporting systems truly uphold confidentiality, anonymity, and protection from retaliation, particularly in gender-based cases;

   II. conduct gender-sensitive impact assessments to evaluate whether whistleblower protections effectively support women, LGBTQ+ individuals, and other vulnerable groups;

   III. establish a feedback mechanism where whistleblowers can anonymously report issues with the system, ensuring continuous improvement.

These measures will help assess the effectiveness of gender-sensitive protections within the whistleblowing system, ensuring that the system is continuously evolving to better protect all whistleblowers, particularly those reporting gender-based misconduct.

Ch. 1 >

FINAL RECOMMENDATIONS

What can be recommended based on the empirical studies?

1. CONDUCTING REGULAR EMPIRICAL STUDIES

Taking into account the empirical study carried out in Poland (2.3), it can be recommended that similar studies be carried out on a regular basis across Member States in order to collect relevant data and build up theoretical and empirical knowledge on the perception and effectiveness of whistleblowing systems in different organisational and national contexts. This would make it possible to monitor the systems' development and continuously improve their effectiveness.

2. ADAPTING THE INDEX FOR EVALUATION OF WHISTLEBLOWER PROTECTION (IEWP)

The Index for Evaluation of Whistleblower Protection – IEWP (2.4) can be taken into account and adapted by Member States when they develop their own assessment indicators. While the IEWP is based on public sector research, it can be adapted to track and assess irregularity reports in the private and non-profit sectors, thereby effectively covering all forms of corruption and institutional malpractice.

3. IMPLEMENTING KEY TI RECOMMENDATIONS FOR WHISTLEBLOWING SYSTEMS

When setting up and maintaining an internal whistleblowing system, some key recommendations from TI (2.5) need to be taken into account. These include ensuring that the system complies with national legal requirements (whistleblower protection laws and other relevant laws such as data protection or labour laws), that it is inclusive and gender-sensitive, that it is formally reviewed at least once a year, and that appropriate changes are made to improve its effectiveness.

RECOMMENDATIONS ON GENDER AND OPEN GOVERNMENT

Chapter 6

6.1 GENDER FOCUS

There is the need for the effective implementation of public whistleblower protection policies that integrate **gender-sensitive channels** at both organizational and external levels. It is essential to address the gaps in existing regulations, such as the EU Directive on Whistleblower Protection and national existing legal framework, which do not explicitly consider **gender-related aspects.**

In this sense

A. international, national and subnational regulatory frameworks should reinforce measures to **establish tailored protection mechanisms for women** whistleblowers and other vulnerable groups;

B. ensuring that **reporting channels are accessible**, inclusive, and responsive to their specific needs and risks;

C. strengthen data collection and analysis mechanisms ensuring a more accurate understanding of whistleblowers' behavior, needs, and priorities;

D. implementing **gender-sensitive channels and targeted policies** would enhance the effectiveness of support processes, particularly for women and other vulnerable groups. Ensuring that procedures for reporting, investigating and resolving complaints are equipped to handle intersectional inequalities;

E. **strengthen gender-sensitive security and confidentiality measures in whistleblowing systems**. Ensure reporting systems include tailored protections for gender-based misconduct, safeguarding whistleblower anonymity and preventing retaliation, especially in power-imbalanced situations;

F. implement confidentiality protocols to secure gender-based reports, protecting identities and preventing indirect identification;

G. develop a **Training and Sensitization on Gender-Sensitive Whistleblowing** as a preventive measure to educate all participants in whistleblowing practices, on gender and the intersection of other vulnerability factors.

The program should :

A. address the reporting of **harassment, sexual abuse**, and corruption-related misconduct;

B. highlight the **differing impacts on women and men**, particularly the disproportionate burden on women;

C. emphasise the **prevention of retaliation**, such as sexual harassment or sextortion, and raising awareness about gender stereotypes, biases, and the specific vulnerabilities that impact whistleblowers in marginalized situations.

6.2 THE OPEN GOVERNMENT (OG) FOCUS

We call for the effective implementation of whistleblower protection policies that integrate open government principles such as transparency, participation, accountability, and inclusion. It is essential to address the gaps in existing regulations and practices, particularly where whistleblowing systems remain unclear, inaccessible, or poorly supported by both institutions and civil society.

In this sense:

A. international, national and subnational frameworks should reinforce **multi-stakeholder collaboration to co-design and monitor whistleblowing systems**, combining institutional perspectives with the experiences and expertise of civil society organizations (CSOs), to ensure clarity, accessibility, and trust in the reporting process;

B. institutional and civic stakeholders should work together to ensure that **reporting channels are understandable, inclusive, and designed with the user in mind**, by using plain language, practical examples, and clear instructions throughout the reporting journey, including repeated guidance and user-friendly forms;

C. strengthen data collection and analysis mechanisms on whistleblowing practices, ensuring **data is published in open formats and used to inform policy** through transparent stakeholder dialogues and iterative improvement cycles;

D. **implement training and support systems for public officials and internal report handlers**, moving beyond a purely legalistic approach to include experiential learning based on ethical dilemmas and real-life case simulations, in collaboration between public authorities and CSOs;

E. **develop joint communication campaigns to raise public awareness** about whistleblower rights and available support services, leveraging national media, cultural platforms, and sports events to reach diverse audiences;

F. **promote participatory risk assessments to identify potential misconduct areas** relevant to whistleblowing within institutions, involving both internal actors and civil society to ensure systems are tailored and context-sensitive;

G. **establish strong data protection guidelines co-developed by data protection authorities and support organizations**, ensuring that advisory services can process personal data in a meaningful yet secure way, balancing privacy with effective support;

H. **co-design new laws or regulations to expand protection mechanisms** to include not only whistleblowers but also those who assist them, such as support CSOs, legal advisors, and journalists, ensuring they are shielded from retaliation, in line with international best practices and human rights frameworks;

I. **create and maintain public registries of civic and institutional information centers**, defining clear inclusion criteria and fostering coordination among listed organizations to refer whistleblowers effectively and monitor systemic challenges through regular peer exchange.

BEYOND THE TOOLKIT

A crucial aspect emerged: **the regulatory framework** has been improved thanks to the EU directive and its conversion into national laws, and other reforms – some of them are included in the recommendations at the end of the previous chapters – can further improve their expected impact on the desired good governance.

Such **"top-down" policy** commitment on whistleblowing, however, needs strong foundations to produce any significant impact on the **complex social** and institutional environment where opportunities for corruption and other malfeasances continuously emerge. Those bases are grounded in values, principles, expectations, beliefs: in other words, the cultural dimension is crucial to "empower" informal norms and shared judgements, socially encouraging and supporting whistleblowing as a normal and valuable component of a desirable **speak-up culture**. The cultural traits which prevail within certain organizations or societies, in fact, decisively impacts the effectiveness of any **whistleblowing** implementation. Especially in environments where corruption and wrongdoings are normalized as unwritten rules, social pressure against whistleblowers may be the dominant and successful attitude. Culture cannot be changed by decree, obviously, but reforms of formal regulation provide signals which address social changes: they can "start a slow-moving process", which over time may generate profound modifications in the way individuals perceive and judge their own and others' conducts. The whistleblower's paradoxical dilemma, if portrayed as "**hero or traitor**", precisely reflects the resistance to ***normalise*** **the practice** of reporting potential wrongdoings in the public interest, making stronger the connection between approaches "whistleblowing-oriented" and "whistleblower-oriented", i.e., between the formal/institutional dimension and the subjective and value-oriented perspective.

To make whistleblowing effective, a careful balance has to be found between conflicting interests, expectations and rights of the different actors involved in the process – the whistleblower being only one of them. The substantial challenges associated with any whistleblowing regulatory framework have been clearly highlighted in the previous chapters. How to **minimize risks** of retaliation, how to safeguard rights to privacy and **protect sensitive** data, how to **verify the content** of whistleblowing reports, for instance, are complex issues. The digital innovations present both opportunities and challenges: online platforms and secure communication tools can facilitate **anonymous reporting** and enhance the protection, but they also **raise concerns about data security** and the potential for misuse. Balancing the benefits of digital tools with the need to protect sensitive information is a **critical issue**. In other words, no universal and fit-for-all formula can be imposed here: regulation on whistleblowing should enable any public or private organization – with its own characteristics and background – towards the tailoring of its particular and context-specific mix of encouragement, constraints, education, enforcement.

Whistleblowing holds immense potential as an anti-corruption tool. Its effectiveness, however, depends on addressing these challenges. An in-depth empirical analysis on the moral and motivational foundations of whistleblowers' reporting seems a necessary source of knowledge for improving the **perceived effectiveness** of the corresponding policies.

Moreover, it should be explored the role of ethical training and educational tools. The latter, in fact, should be effective to increase the congruence of individuals' values, in which they are socialised in the circles of social recognition within public and private organisations, with rules and procedures oriented towards the public interest. When a certain **societal stigma** towards the whistleblower's role prevails, even the most sophisticated platforms for confidential or anonymous reporting will be useless. A persevering activity of '**ethical training**' within public apparatuses, as well as private organisations, could assume a **crucial role** here. Such commitment should be aimed at strengthening social circuits of mutual recognition and **positive 'reinforcement'** of loyalty towards the public and private organisations' aims, consolidation moral barriers against corruption and the ethical motivations for reporting wrongdoings.

In conclusion, it appears necessary to **reconsider the social dimension** within which the sources of moral recognition, which are the main driving force behind the decision to "open the whistle" are being shaped over time. After all, the success of whistleblowing regulation and legislation depends primarily on its coordination within a broader anti-corruption collective action "**from below**", involving all the most important social circles - in the working environment as well as in the professional, associative, political, trade union, religious spheres. Only the latter, in fact, can generate the ferment for a **cultural change**, i.e. a binding framework of beliefs and informal norms where whistleblowing is encouraged and mutually supported through the public expression of positive ethical judgments on its socially beneficial effects.

ANNEX I : RESEARCH METHODOLOGY AND DATA COLLECTION

This toolkit is the result of each partner expertise in the field and a research conducted with mixed methods from June 2024 until November 2024 in four key phases:

1. Desk review and literature research

In this phase it has been established a conceptual and regulatory framework of whistleblower protection, assessing obligations, level of implementation, and loopholes.

2. Stakeholder analysis and mapping

In this phase, fifty primary stakeholders among civil society organisations (Cso), authorities, private sector, media, official order academia and trade unions have been identified and mapped. Those are the actors that could influence or are important to promoting whistleblowing legislation and awareness. The stakeholder database has been the base to prepare a list of organisations for qualitative research and interviews.

3. Expert key informant interviews

In this phase representatives of at least five organisations per country have been interviewed to gather insights about challenges, opportunities, recommendations and guidelines. The script of the interviews has been based on the topics of the toolkit, however the method used is semi-structured key informant interviews, to adapt to the interviewees' responses. This is particularly useful for exploring innovative and comprehensive practices that might not have been considered during the design. Each interviewer has received a formal consent agreement to fully comply with data protection. Audio recordings have been produced.

4. Analysis

The interviews were analyzed using a summary format, which links the interview content to each chapter and highlights the following key themes:

A. existing best practices, either implemented by the interviewed organization or cited by it;
B. needs and challenges identified by the interviewee related to the chapter topic;
C. proposals or key points for action to improve the current situation.

Furthermore, the main topics emerged from the interviews, have been collected and summarised in an excel file. Indeed, the references and quotations in the text are taken from the interviews with experts conducted for the purpose of this guide.

ANNEX II : ACRONYMS

ANAC: Autorità nazionale anticorruzione

CAWI: Computer-Assisted Web Interviewing

CATI: Computer-Assisted Telephone Interviewing

CPDP: Commission for Personal Data Protection/ Комисия за защита на личните данни

CSO: Civil Society Association

DPO: Data protection officer

DSA: Digital Services Act

ECHR: European Convention on Human Rights

EU: European Union

GCB: Transparency International's Global Corruption Barometer

GDPR: General Data Protection Regulation

NGO: Non Governmental Organisation

IEWP: Index for Evaluation of Whistleblower Protection

OECD: Organisation for Economic Co-operation and Development

OG: Open Government

OGP: Open Government Partnership

SLAPP: Strategic Lawsuits Against Public Participation

SNA: National School of Administration

TFEU: The Treaty on the Functioning of the European Union

UN: United Nations

UNODC: United Nations Office on Drugs and Crime

WHO: World Health Organisation

WCAG: Web Content Accessibility Guidelines

W3C: World Wide Web Consortium

WMS: Whistleblowing Management Systems

Open the whistle

Whistleblowing Integrity

TOOLKIT

Co-funded by
the European Union