TRANSPARENCY INTERNATIONAL
the global coalition against corruption

INTERNAL WHISTLEBLOWING SYSTEMS

Best practice principles for public and private organisations

Transparency International is a global movement with one vision: a world in which government, business, civil society and the daily lives of people are free of corruption. With more than 100 chapters worldwide and an international secretariat in Berlin, we are leading the fight against corruption to turn this vision into reality.

www.transparency.org

Internal whistleblowing systems

Best practice principles for public and private organisations

Author: Marie Terracol

Cover: Comaniciu Dan / Shutterstock

ISBN: 978-3-96076-227-0

Funded by the European Union

This publication was produced as part of the "Speak Up Europe" project, which was funded by the European Union's Internal Security Fund — Police. The content of this publication represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

TABLE OF CONTENTS

Acknowlegements **4**

Glossary **5**

Introduction **6**

Objectives of an internal whistleblowing system 7

Who should implement internal whistleblowing systems? 8

Key considerations when setting up an internal whistleblowing system 9

Key principles for internal whistleblowing systems **11**

Scope **14**

What type of wrongdoing should be covered by internal whistleblowing systems? 14

Who should be able to report through internal whistleblowing systems? 16

Who should be protected? 17

Roles and responsibilities **18**

Top leadership 18

The whistleblowing officer or office 19

Line managers 20

Personnel 20

Information and communication **21**

Information to all relevant stakeholders 21

Accountability to stakeholders through transparency and public reporting 23

Procedures **25**

Multiple whistleblowing channels 25

Taking action on whistleblowing reports 27

Record-keeping and data protection 30

Support and protection for whistleblowers **32**

Protecting the identity of whistleblowers and other protected persons 32

Protection from detrimental conduct and interference 34

Addressing detrimental conduct, interference and breaches of confidentiality 36

Supporting whistleblowers 38

Protection of the person concerned **39**

Continuous monitoring and review **40**

References and resources **42**

Resources from Transparency International 42

Other resources 43

ACKNOWLEGEMENTS

The author and Transparency International would like to thank the following individuals and organisations who provided insight and expertise that greatly assisted the development of these best-practice principles for internal whistleblowing mechanisms.

AJ Brown, Transparency International and Griffith University
Alexandra Konstantinova, Transparency International Bulgaria
Andrew Pepper-Parsons, Protect
Anoukh de Soysa, Transparency International
Camillo Rubiano, Public Services International
Celine Pinzio, Transparency International
Claire Launay, Transparencia por Colombia
David Lewis, Middlesex University London
David Martinez, Transparency International España
Elizabeth Gardiner, Protect
Flora Cresswell, Transparency International
Giorgio Fraschini, Transparency International Italia
Indira Alexandra Ricaurte Villalobos, Transparencia por Colombia
Jane Olsen, Griffith University
John Devitt, Transparency International Ireland
Kush Amin, Transparency International
Laurence Fabre, Transparency International France
Linda Ofori-Kwafo, Ghana Integrity Initiative
Lotta Rydstrom, Transparency International Sweden
Lotte Rooijendijk, Transparency International Netherlands
Samantha Nurick, Transparency International
Sebastian Oelrich, Transparency International Germany
Stephanie Casey, Transparency International Ireland
Tom Devine, Government Accountability Project
Vasja Cepic, Transparency International Slovenia

GLOSSARY

Whistleblowing: communicating information on suspected wrongdoing (see below) to individuals or entities believed to be able to effect action.

Wrongdoing: an act or omission that is unlawful, abusive or can cause harm.

Whistleblower: any person reporting or disclosing suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting.

Internal report: a whistleblowing report made within a public or private organisation (i.e. within the workplace).

External report: a whistleblowing report made to a competent authority.

Public disclosure: making information on breaches available in the public domain, either by publishing the information – for example, on online platforms or social media – or by reporting it to stakeholders such as the media, elected officials, civil society organisations, legal associations, trade unions or business/professional organisations.

Detrimental conduct: any threatened, recommended or actual act or omission, direct or indirect, which causes or may cause harm, and is linked to or resulting from actual or suspected whistleblowing.

Person concerned: a natural or legal person who is referred to in a whistleblower's report or complaint as a person responsible for the suspected wrongdoing or detrimental conduct, or associated with that person.

Personnel: an organisation's directors, officers, employees, temporary staff or workers, and volunteers.[1]

Personnel representatives: persons who are recognised as such under national law or practice, whether they are trade union representatives or elected representatives (e.g. works councils).

[1] ISO 37002:2021, Whistleblowing management systems — Guidelines.

INTRODUCTION

Whistleblowing is one of the most effective ways to uncover corruption, fraud, mismanagement and other wrongdoing that threaten public health and safety, financial integrity, human rights and the environment.

Whistleblowing is the disclosure of information about suspected wrongdoing to individuals or entities believed to be able to effect action. Organisations themselves are often best placed to deal with wrongdoing occurring within their remit, and in practice, most whistleblowers first report such suspected wrongdoing within their organisation. It is therefore essential that organisations, whether private companies or public institutions, provide safe and effective mechanisms to receive and address these reports, as well as robust protection to whistleblowers.

Consequently, an increasing number of national laws require organisations to implement internal whistleblowing systems (IWS), also known as "speak up" or internal reporting systems. This has been the case since December 2021 in EU countries, for example, under the EU Whistleblower Protection Directive.

But organisations should not consider IWS as just a legal obligation. Effective IWS help protect organisations from the effects of misconduct – including legal liability, lasting reputational harm and serious financial losses. By enabling personnel and other relevant stakeholders to speak up about unethical or illegal conduct, IWS foster an organisational culture of trust, transparency and accountability. They therefore provide real benefits to an organisation's culture, brand, value creation and growth.[2]

This publication aims to support organisations' implementation of effective internal whistleblowing systems. It also seeks to help organisations operating within the EU to meet their obligations under the EU Directive on Whistleblower Protection.

The principles below provide guidance on IWS best practice, in compliance with the EU Directive on Whistleblower Protection and the ISO Guidelines for Whistleblowing Management Systems.[3] They offer support to:

- organisations across all sectors (public, private and "third" sectors) and jurisdictions (including international organisations such as the United Nations) in designing and implementing IWS.
- policymakers developing regulations, administrative provisions and national guidelines on IWS.

[2] See for example Stephen Stubben and Kyle Welch (2020), Evidence on the Use and Efficacy of Internal Whistleblowing Systems; Bussmann, K.-D., & Niemeczek, A. (2019), Compliance through company culture and values: An international study based on the example of corruption prevention. *Journal of Business Ethics*, 157(3), 797–811; Kaptein, M. (2011), From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing, *Journal of Business Ethics*, 98, 513–530; Mayer, D.M., Nurmohamed, S., Klebe Treviño, L., Shapiro, D.L., & Schminke, M. (2013), Encouraging Employees to Report Unethical Conduct Internally: It Takes a Village. *Organizational Behavior and Human Decision Processes*, 121, 89-103; Seifert, D. L., Sweeney, J. T., Joireman, J., & Thornton, J. M. (2010). The influence of organizational justice on accountant whistleblowing. *Accounting, Organizations and Society*, 35(7), 707-717.

[3] It should be noted that while the principles below meet, at a minimum, the standards set in the EU Directive on Whistleblower Protection and in the ISO Guidelines for Whistleblowing Management Systems. In several instances they go beyond these standards to meet best practice.

- CSOs and other actors, such as business associations and trade unions, seeking to ensure that organisations implement effective IWS, e.g. through advocacy or by developing IWS tools tailored to their national contexts.

OBJECTIVES OF AN INTERNAL WHISTLEBLOWING SYSTEM

- Empower personnel and other relevant stakeholders to speak up about wrongdoing.
- Enable timely detection and diligent address of wrongdoing committed, within, by or for the organisation.
- Prevent and minimise damage to the organisation, including legal liability, serious financial losses and lasting reputational harm resulting in decreased public trust, by enabling early detection and correction of wrongdoing.
- Prevent and minimise damage to the public interest, including public health, human rights and the environment.
- Protect whistleblowers and third parties at risk of detrimental conduct.
- Enable the organisation to learn and remediate.
- Foster an organisational culture of trust, transparency and accountability, which helps prevent wrongdoing.

Benefits of Internal Whistleblowing Systems

Internal whistleblowing systems provide real and highly valuable benefits to organisations of all types:

1. A public signal of commitment to integrity and social responsibility

Shareholder demands for effective internal ethics programmes to support long-term value creation are growing. Internal reporting systems signal to investors and the public that an organisation prioritises risk management, social responsibility and integrity.

2. Prevention and mitigation of liability

Early detection gives organisations the opportunity to address wrongful conduct before a situation escalates to trigger liability. It also provides an opportunity to voluntarily self-report to relevant regulatory agencies, before an agency initiates action and reaches an adverse conclusion because the organisation failed to act.

3. Prevention and mitigation of financial losses

Internal reporting systems can prevent or mitigate financial losses from fraud and liability, such as civil or criminal penalties. Knowledge that a reporting system exists can discourage individuals from misconduct through fear of being reported.[4]

4. Continuous improvement in compliance and risk management

Information on issues raised through an internal reporting system enables organisations to improve their policies and procedures, and identify where more resources are needed to reduce risk exposure.

[4] Jaron H. Wilde; The Deterrent Effect of Employee Whistleblowing on Firms' Financial Misreporting and Tax Aggressiveness. *The Accounting Review*, 1 September 2017; 92 (5): 247–280; The Institute of Internal Auditors, the American Institute of Certified Public Accountant, ACFE, Managing the Business Risk of Fraud: A Practical Guide, p.35.

5. Strengthening of reputation

An ethical breach or legal violation can destroy an organisation's brand value, with severe consequences, including lower investment, lost profits and low morale among personnel. With internal reporting, leaders can prevent or mitigate reputational damage.

6. Enhancement of organisational culture

Backed by encouragement from leaders and corporate responsiveness to reports of misconduct, internal reporting systems can build an organisational culture of trust, transparency and accountability, with a positive impact on personnel performance and retention.

Source: Transparency International, The Business Case for 'Speaking Up': how Internal Reporting Mechanisms Strengthen Private-Sector Organisations, 2017

WHO SHOULD IMPLEMENT INTERNAL WHISTLEBLOWING SYSTEMS?

All public and most private organisations should have an internal whistleblowing system.

All public organisations

- All public entities, at local, regional, national or international level, without exception and regardless of size, should implement IWS (albeit in ways appropriate to their size).[5] This includes entities that are publicly owned or controlled, such as state-owned enterprises.

Most private organisations[6]

- All medium-sized and large private entities (with 50 or more employees), as well as all entities in the financial service industry, irrespective of size,[7] should implement IWS. This includes both companies and non-profit organisations.
- Small private entities (with less than 50 employees) are strongly advised to implement IWS, especially when the nature of their activities presents risk to the public interest (for example, to human rights, the environment or public health). Companies that are part of a corporate group should have IWS regardless of their size.[8]
- Small and medium-sized private entities (with less than 250 employees) could opt to share resources for the receipt of reports and any subsequent investigation. However, the responsibility to maintain confidentiality, give feedback to the whistleblower and address the reported wrongdoing remains with each organisation concerned.

[5] Even small municipalities routinely take decisions in high-risk areas such as public procurement, environmental protection and public health, making the presence of IWS critical. The EU Directive allows municipalities to have shared or joint whistleblowing channels, but they still need to implement their own IWS for all other aspects.
[6] Private organisations include organisations from the third sector, i.e. not-for-profit organisations such as civil society organisations, charities and non-governmental organisations.
[7] This is due to the particular risks of money laundering and terrorist financing. Most private entities providing financial services, products and markets in the EU are required to implement IWS by various EU Directives.
[8] As smaller entities of the group can easily share resources for the receipt of reports and any investigation to be carried out – for example, through the group-level IWS – the potential administrative and financial burden of implementing an IWS is small and greatly outweighed by its benefits to the organisations and the public interest.

- All private entities, including those that have not implemented IWS, should protect whistleblowers against detrimental conduct.

KEY CONSIDERATIONS WHEN SETTING UP AN INTERNAL WHISTLEBLOWING SYSTEM

- IWS should be commensurate to the organisation's size and its exposure to risks of wrongdoing. Organisations should therefore undertake a risk and needs assessment to inform their IWS design.
- IWS form part of the organisation's governance framework and are often embedded in, or at least linked to, integrity and compliance programmes. They are different from human resources (HR) or grievance procedures.[9]
- IWS should be designed following consultation with relevant stakeholders at all levels, both internal and external – and, where appropriate, in agreement with them. These include employees, works councils, trade unions or other personnel representatives.
- IWS should comply with national legal requirements. This includes whistleblower protection legislation, but also other legislation, such as data protection or labour laws.
- IWS should be inclusive and gender sensitive.[10]

EU Whistleblower Protection Directive

In 2019, the European Union adopted the "Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law" (Whistleblower Protection Directive). The 27 EU member states had two years until December 2021 to comply with the directive, although most did not meet the deadline.[11]

The directive provides strong common minimum standards for the protection of whistleblowers in Europe. Member states should transpose these provisions in line with the spirit of the directive, which is to provide a high level of protection for whistleblowers.

Key provisions of the EU Whistleblower Directive:

- The directive covers both the public and private sectors.
- It covers a wide range of potential whistleblowers, including individuals outside the traditional employee-employer relationship, such as consultants, contractors, volunteers, board members, former workers and job applicants (Article 4).
- It also protects individuals who assist whistleblowers, as well as individuals and legal entities connected with whistleblowers (Article 4.4).
- Breaches of law are defined as acts or omissions that are either unlawful or that defeat the object or the purpose of the rules (Article 5.1).

[9] See "Articulation between IWS and other internal reporting systems" in the section on Scope.
[10] See Transparency International (2021), "Finding a voice, Seeking Justice – The barriers women face to reporting corruption in the European Union", position paper; Nieves Zúñiga (2020), "Gender Sensitivity in Corruption Reporting and Whistleblowing", U4 Helpdesk Answer.
[11] See the EU Whistleblowing Monitor to follow the progress of transposition of the EU Directive on Whistleblowing across all 27 EU member states, www.whistleblowingmonitor.eu/.

- In granting protection, the directive does not in any way take into account the whistleblowers' motive for reporting.
- It protects the identity of whistleblowers in most circumstances, with clear and limited exceptions to confidentiality, and advance notice to the whistleblower when their identity needs to be disclosed (Article 16).
- It grants protection to whistleblowers who have reported or disclosed information anonymously and have subsequently been identified (Article 6.3).
- It places an obligation on a wide range of public and private entities to establish internal whistleblowing systems (Article 8).
- It establishes an obligation for public and private entities and competent authorities to follow up on reports received and to keep the whistleblower informed within a reasonable timeframe (Articles 9 and 11.2).
- It allows whistleblowers to report breaches of law internally or directly to the competent authorities (Article 10).
- It allows for public disclosures in certain circumstances (Article 15).
- It prohibits "any form of retaliation", including threats of retaliation and attempts at retaliation, and provides a long, diverse and non-exhaustive list of examples (Article 19).
- It requires EU member states to ensure that easily accessible and free, comprehensive and independent advice is provided to the public (Article 20.1(a)).
- It foresees legal and financial assistance to whistleblowers, which are essential elements of effective whistleblower protection (Article 20.2).
- It creates a presumption of retaliation when a whistleblower suffers detriment (Article 21.5).
- It provides for interim relief which enables a whistleblower to maintain professional and financial status until legal proceedings end (Article 21.6).
- It provides for penalties to be applied to persons who hinder or attempt to hinder reporting, retaliate against whistleblowers (including by bringing vexatious proceedings) or breach the duty of maintaining confidentiality over the whistleblowers' identity (Article 23).
- It provides that whistleblowers cannot be held liable for breaching restrictions on the acquisition or disclosure of information, including for breaches of trade or other secrets (Article 21(2)(3)(7)). It also excludes the possibility of contracting out of the right to blow the whistle – for example, through loyalty clauses or confidentiality or non-disclosure agreements (Article 24).

KEY PRINCIPLES FOR INTERNAL WHISTLEBLOWING SYSTEMS

1. All public and most private organisations should have an internal whistleblowing system, following these key principles:

SCOPE

2. Internal whistleblowing systems should invite reports regarding any suspected wrongdoing – that is any act or omission that is unlawful, abusive or can cause harm – committed in, by or for the organisation.

3. Internal whistleblowing systems should invite reports from any person who might acquire, in the context of their work-related activities, information on wrongdoing committed in, by or for the organisation.

4. Organisations should protect whistleblowers – that is, any persons reporting suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting – as well as third parties at risk of detrimental conduct.

ROLES AND REPONSIBILITIES

5. The organisation's top leadership are responsible and accountable for the effective implementation of its internal whistleblowing system. They should demonstrate their commitment and set a clear "tone from the top" in support of speaking up and listening up about wrongdoing.

6. Organisations should designate an impartial person or department responsible for the operation of the internal whistleblowing system. This person or department should be free from conflict of interest, and have sufficient independence, powers and resources, as well as the relevant qualifications.

INFORMATION AND COMMUNICATION

7. Information about the organisation's internal whistleblowing system should be highly visible and accessible, via a wide range of media and channels. All relevant stakeholders, including all potential whistleblowers and persons concerned, should have access to and receive relevant information on the internal whistleblowing system.

8. Organisations should report publicly every year on their commitment to a "speak up and listen up" culture and the implementation of their internal whistleblowing system.

PROCEDURES

9. Internal whistleblowing systems should include multiple reporting channels that are safe and easily accessible, and enable reporting in writing and orally. Organisations should recognise line managers as possible recipients of whistleblowing reports.

10. Internal whistleblowing systems should ensure diligent – that is, thorough, timely, fair and impartial – follow-up of all reports received,[12] in order to establish whether wrongdoing occurred,[13] to address confirmed wrongdoing and to correct any systemic issue identified. The follow-up of a report should involve the meaningful participation of the whistleblower.

11. As knowledgeable and interested stakeholders, whistleblowers should be kept informed throughout the process and have meaningful opportunities to provide input to the follow-up of their report.

12. Reports received, actions taken as follow-up, and the findings and outcome of the follow-up, as well as communication with the whistleblower and concerned person, should be adequately documented and kept in retrievable and auditable form in accordance with confidentiality and data protection requirements.

SUPPORT AND PROTECTION FOR WHISTLEBLOWERS

13. Without the explicit consent of the whistleblower, their identity and any identifying information – that is, information from which the identity of the whistleblower may be directly or indirectly deduced – should not be disclosed beyond those persons competent to receive or follow up on reports.

14. Organisations should accept and follow up on anonymous reports, and protect anonymous whistleblowers.

15. Organisations should prohibit any form of detrimental conduct – that is any threatened, recommended or actual act or omission, direct or indirect, which causes or may cause harm – linked to whistleblowing, and any interference with whistleblowing.

[12] This includes anonymous reports.
[13] Or is occurring or is like to occur.

16. Organisations should take reasonable steps to prevent detrimental conduct and to ensure that individuals and entities under their control or working for them refrain from detrimental conduct.

17. Internal whistleblowing systems should provide for enforceable, transparent and timely mechanisms to (1) receive and follow up on complaints of detrimental conduct, interference and breach of confidentiality, (2) sanction perpetrators and (3) ensure full reparation of affected whistleblowers and other protected persons via remedial measures and compensation.

18. Organisations should provide support to whistleblowers to prevent harm to their health or career.

PROTECTION OF PERSON CONCERNED

19. Organisations should protect the identity and the rights of the person concerned, including by providing for effective, proportionate and dissuasive sanctions for individuals who knowingly report false information.

CONTINUOUS MONITORING AND REVIEW

20. Internal whistleblowing systems should be formally reviewed at least annually, and revisions should be made accordingly to improve effectiveness and ensure systems are up to date and in line with legislation and best practice.

SCOPE

Organisations should clearly define who can report and what can be reported – and addressed – through their IWS, as well as who should be protected.

WHAT TYPE OF WRONGDOING SHOULD BE COVERED BY INTERNAL WHISTLEBLOWING SYSTEMS?

Internal whistleblowing systems should invite reports regarding any suspected wrongdoing committed in, by or for the organisation.

- Wrongdoing should be understood as any act or omission that is unlawful, abusive or can cause harm. This includes, but is not limited to:
    - corruption in all its forms (including bribery, money laundering or sextortion)
    - criminal offences
    - breaches of legal obligation (national and international)
    - dangers to public and occupational health and safety
    - dangers to the environment
    - human rights violations
    - child exploitation or abuse
    - sexual harassment, bullying and discrimination
    - animal abuse, neglect or cruelty
    - miscarriages of justice
    - abuse of authority
    - insider trading, tax evasion or breaches of antitrust law and international trade sanctions
    - unauthorised use of funds, property or resources
    - gross waste or mismanagement
    - conflict of interest
    - fraudulent financial disclosures
    - detrimental conduct against whistleblowers and other protected parties

    - improper behaviour that seriously harms or is likely to seriously harm the reputation or financial wellbeing of the organisation
    - any other violation of the organisation's code of conduct or code of ethics and relevant policies
    - concealment of wrongdoing and attempts to conceal such wrongdoing, including hindering or attempting to hinder whistleblowing.
- Breaches of a whistleblower's own contract with the organisation, such as an employment contract, consultancy contract or service contract, are not usually included in the scope of wrongdoing reportable through IWS. Unless they also constitute wrongdoing as defined above, complaints about such breaches will typically be handled by other systems, such as the HR grievance process (see box on "Articulation between IWS and other internal reporting systems" below).
- IWS should invite reports regarding suspected wrongdoing committed by anyone working directly or indirectly for the organisation, or under any form of contract or agreement with it, including current and former employees, executive personnel, board members, interns, student workers, volunteers, contractors, sub-contractors, suppliers or consultants, in the context of their work within or for the organisation.
- IWS should invite reports relating to suspected wrongdoing that has been, is being or is likely to be committed.
- IWS should not exclude reports involving information such as the organisation's trade secrets or unpublished financial information.
- Organisations dealing with matters of national security, official or military secrets, or classified information should not exclude reports involving these categories of information from their IWS. Rather, they may consider establishing special channels to receive reports involving matters of national security, official or military secrets, or classified information, staffed with personnel entitled to receive and handle such information.

Articulation between IWS and other internal reporting systems

Organisations often have other reporting or complaint systems alongside their internal whistleblowing system, typically to address personnel and workplace grievances. The articulation between these systems can be challenging, with their scope often overlapping – for example, regarding harassment and discrimination, data protection, or occupational health and safety violations – and the issues reported often being complex and involving several types of wrongdoing. The procedures, methods of investigation, and rights and obligations of the organisation and the reporting person might also differ depending on the reporting or complaint system.

- Organisations should offer guidance about which reporting or complaint system is best-suited to receive and handle which types of concern. The availability of clear information, such as FAQs, as well as awareness training is key to effectively guiding individuals toward the most appropriate channel.
- Organisations should not be too prescriptive and strict regarding which internal channel a person should use, to avoid discouraging people from raising their concerns. The choice of channel should be with the reporting party.
- If, after an initial assessment, it appears that another reporting or complaint system might be more appropriate, the reporting person can be directed by the person handling the report to that other channel. Reports should not be transferred to the person or department handling another reporting system without the explicit consent of the individual who raised the concern.

- Reports with mixed or unclear scope should be managed through the system chosen by the reporting person, in coordination with other relevant systems, where appropriate.[14]

WHO SHOULD BE ABLE TO REPORT THROUGH INTERNAL WHISTLEBLOWING SYSTEMS?

Internal whistleblowing systems should invite reports from any person who might acquire, in the context of their work-related activities, information on wrongdoing committed in, by or for the organisation.

- This includes at least the following categories of individuals, whether their relationship with the organisation is current or has ended:
    - workers (whether full- or part-time, fixed-term or temporary), including civil servants
    - self-employed persons
    - shareholders and persons belonging to the administrative, management or supervisory body
    - volunteers and paid or unpaid trainees
    - persons working under the supervision and direction of contractors, sub-contractors and suppliers
    - persons who acquired information during the recruitment process or other pre-contractual negotiations, such as job applicants or bidders.
- Organisations might also consider opening their internal whistleblowing system to any person who might acquire information on wrongdoing committed in or by the organisation, including outside the context of their work-related activities, such as users, customers, beneficiaries or local community members. Alternatively, organisations could consider implementing separate systems to receive and handle reports from "outsiders".[15]
- When deciding which categories of person should be able to report through their IWS – such as employees, volunteers, sub-contractors' workers, users or beneficiaries – organisations should carefully consider, for each category of persons, the forms of detrimental conduct they could suffer from and how the organisation will protect and support them and provide clear information in that regard.

[14] For example, if a person chooses to report sexual harassment through the grievance procedure, the person(s) in charge of handling grievance cases (generally human resources personnel) should inform the reporting person that their case might also fall within the scope of the IWS and, with the consent of the reporting person, inform and involve the whistleblowing officer in the follow-up of the report, if relevant. This is to avoid duplicate or parallel case management, and ensure clarity regarding roles and responsibilities, as well as information exchange, as appropriate.

[15] Before enabling "outsiders" to report through its IWS, the organisation should consider how protection can be afforded to them, and provide clear information in that regard.

WHO SHOULD BE PROTECTED?

Organisations should protect whistleblowers – that is, any persons reporting suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting – as well as third parties at risk of detrimental conduct.

Whistleblowers

- Whistleblowers are any persons reporting suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting.
- "Reasonable belief" means someone with equivalent knowledge, education and experience (a peer) could agree with such a belief. Organisations should protect whistleblowers regardless of whether any subsequent investigation finds proof of wrongdoing, including those who reported inaccurate information in honest error. Whistleblowers are rarely in a position to know the full picture, so their belief might not be accurate.
- Organisations should protect whistleblowers without any consideration of their motives for reporting.
- Organisations should protect whistleblowers whether they reported internally or externally to the authorities or made a public disclosure.
- Organisations should protect whistleblowers who have reported information anonymously and have subsequently been identified.
- Organisations should protect whistleblowers whether they used the designated internal channels or reported to another "natural" internal authority (such as a manager, health and safety officer, chief compliance officer, HR officer, integrity officer, legal or privacy officer, chief financial officer, chief audit executive or board member). This includes individuals who report wrongdoing in the course of their job duties (so-called "duty speech" or "role-prescribed whistleblowers").[16]

Third parties at risk of detrimental conduct

These include:

- persons who are believed or suspected to be a whistleblower, even mistakenly
- legal entities that the whistleblower owns, works for or is otherwise connected with
- third persons who are connected with the whistleblower, such as colleagues and relatives
- natural persons who assist or attempt to assist a whistleblower
- legal persons, including civil society organisations and trade unions, who assist or attempt to assist a whistleblower
- persons named in the report as potential witnesses
- persons participating in the follow-up of a report (including witnesses)
- persons who refuse to participate in wrongdoing.

[16] Government Accountability Project and International Bar Association (2021), *Are whistleblowing laws working? A global study of whistleblower protection litigation*, p. 13; Kim Loyens and Jeroen Maesschalck, "Whistleblowing and Power: New Avenues for Research", in *International Handbook of Whistleblowing Research*, eds A.J. Brown et al. (Cheltenham: Edward Elgar, 2014), 154–173.

ROLES AND RESPONSIBILITIES

Roles and responsibilities of all those involved in the implementation of the IWS should be clearly established and communicated.

TOP LEADERSHIP

The organisation's top leadership are responsible and accountable for the effective implementation of its internal whistleblowing system. They should demonstrate their commitment and set a clear "tone from the top" in support of speaking up and listening up about wrongdoing.

- The organisation's top leadership – that is, the chair, board members, the head of the organisation and senior management – should set a clear "tone from the top" through internal and public commitments to implementation of the IWS, and to creating and maintaining a "speak up and listen up" culture throughout the organisation.
- Internal whistleblowing systems should be approved by the head of the organisation and endorsed by the board of directors or equivalent body.
- The board of directors or equivalent body should give the head of the organisation overall responsibility for the IWS, who in turn should assign responsibility for operational aspects of the system to the whistleblowing officer or head of the whistleblowing office.
- The board of directors or equivalent body and the head of the organisation should ensure adequate resources are available for effective implementation of the IWS.
- The board of directors or equivalent body should provide diligent oversight of and accountability for the IWS, including by questioning the head of the organisation and the whistleblowing officer or head of the whistleblowing office on the design and implementation of the IWS.
- As part of the monitoring and review process, the board and the head of the organisation should receive regular reports from the whistleblowing officer or head of the whistleblowing office on the IWS operation to assess its effectiveness and suitability.
- Board members, the head of the organisation and senior management should receive relevant training on the IWS.

THE WHISTLEBLOWING OFFICER OR OFFICE

Organisations should designate an impartial person or department responsible for the operation of IWS. This person or department should be free from conflict of interest, and have sufficient independence, powers and resources, as well as the relevant qualifications.

- Depending on their size, risk exposure and needs, organisations should designate a person (the "whistleblowing officer") or department (the "whistleblowing office") as responsible for the operation of the IWS, including for:
    - providing any interested person with information on the organisations' whistleblowing and whistleblower protection policy and procedures
    - receiving reports
    - following up on reports
    - maintaining communication with whistleblowers, including asking for further information where necessary and providing feedback
    - designing, monitoring and reviewing the IWS
    - regularly reporting to the head of the organisation and the board of directors on implementation of the IWS.
- The whistleblowing officer or office should be impartial – that is, free from conflict of interest and with sufficient independence. This may be achieved through the organisational structure, the governance structure and by procedural means, depending on the size of the organisation and the level of resources available.
    - The whistleblowing officer or head of the whistleblowing office should have direct and ready access to the board or equivalent body that oversees the IWS. To provide such access, the whistleblowing officer or head of the whistleblowing office should report directly to both the board and the head of the organisation.[17]
    - The IWS should provide for solutions for potential conflict of interest of the whistleblowing officer or office, for example, through a procedure to handle whistleblowing reports concerning the whistleblowing officer or office themselves.
- The whistleblowing officer or office should be given sufficient resources and authority to fulfil their function effectively.
- Depending on the size and needs of the organisation, the whistleblowing officer may combine that role with another function. In such cases:
    - organisations should pay particular attention to the workload of that individual, to ensure they can allocate adequate time to their whistleblowing officer role.
    - the whistleblowing officer should preferably not have a line management duty towards other employees.

[17] In larger organisations, the whistleblowing officer or head of the whistleblowing office should preferably not be an executive or a board member.

- The whistleblowing officer or members of the whistleblowing office should have the relevant qualifications and receive specific and regular training for the purpose of operating the IWS, including to ensure inclusiveness and gender sensitivity.
- It is important that the persons responsible for handling reports are deemed trustworthy, therefore the organisation should base their designation on criteria including inclusion and diversity.

LINE MANAGERS

- Line managers should also be designated to receive internal whistleblowing reports, as they are the most natural and frequently used channels for reporting work-related issues in daily life.
- Organisations should train line managers in the receipt and handling of whistleblowing reports, addressing issues including:
    - recognising whistleblowing reports
    - the scope of the IWS and the legal framework
    - how to handle the information received, such as maintaining confidentiality, data protection and record keeping
    - how to listen and provide feedback.

  Such training should be delivered regularly, either internally or externally.

PERSONNEL

- Personnel are prohibited from engaging in any form of detrimental conduct against a whistleblower or protected third party.
- Where a report is received through internal channels other than the designated reporting channels or by personnel other than those responsible for handling reports, the personnel who receive the report are prohibited from disclosing any information that might identify the whistleblower or the person concerned, and should promptly direct the whistleblower to the proper channel, where possible.
- Organisations should inform personnel of their responsibilities under the IWS, including via regular awareness training.

INFORMATION AND COMMUNICATION

Information and communication measures are key to ensure awareness among relevant stakeholders and accountability of the organisation regarding the IWS.

INFORMATION TO ALL RELEVANT STAKEHOLDERS

Information about the organisation's IWS should be highly visible and accessible, via a wide range of media and channels. All relevant stakeholders, including all potential whistleblowers and persons concerned, should have access to and receive relevant information on the IWS.

Information to provide

Organisations should provide information that is clear, easily accessible and inclusive,[18] covering the following:

- leadership commitment from the board of directors, head of the organisation and senior management to building the organisation's "speak up and listen up" culture and to the IWS, including commitments to protect whistleblowers, take action in response to whistleblowing reports and train relevant managers and employees.
- how the board provides accountability and oversight of the IWS.
- the organisations' whistleblowing and whistleblower protection policy and procedures, which should include information about:
    - the scope of the IWS, including in relation to other internal reporting or systems
    - the conditions for qualifying for protection
    - contact details for the internal information and reporting channels
    - the procedures applicable to the reporting of wrongdoing, including regarding requests for clarification or further information and feedback to the whistleblower
    - the confidentiality and anonymity regime, including legal exceptions and practical limitations
    - the nature of the follow-up to be given

[18] Clarity and accessibility might require the information to be available in different languages.

    - the type of protection and support measures provided by the organisation to whistleblowers,[19] including the procedures and remedies to address detrimental conduct
    - how personal data will be processed, how long it will be retained and for what purpose.
- the applicable law, including who is protected by national whistleblower protection legislation and how, highlighting potential differences between the organisation's whistleblowing and whistleblower protection policy and procedures and the law, so that potential whistleblowers understand what constitutes their legal protection and what is a voluntary higher commitment by the organisation.
- the contact details of available confidential, independent, free advice channels outside the organisation, such as national authorities, trade unions or civil society organisations.
- the procedures for reporting externally to competent authorities.[20]

Informing the organisation's personnel

- Organisations should signpost IWS in the workplace, both physically and electronically, using a wide range of media and channels, including leaflets, posters and a dedicated section on the organisation's intranet and website.
- Organisations should also regularly promote IWS, for example, at general personnel meetings, in internal newsletters, emails and email signatures, or through a dedicated awareness campaign, such as "Speak Up and Listen Up week").
- Employment contracts should require that all employees read and acknowledge the organisation's code of conduct and whistleblowing and whistleblower protection policy.
- Organisations should provide awareness training to all board directors and employees, at induction and at regular intervals, as they are all potential whistleblowers or persons concerned.

Informing other potential whistleblowers and persons concerned

- Organisations should provide information about their IWS on their website, in an easily accessible, dedicated section, to ensure that all potential whistleblowers or persons concerned have access to relevant information.
- Organisations also should provide tailored communication and, where appropriate, training on their IWS to external stakeholders who are potential whistleblowers or persons concerned, such as consultants, contractors, sub-contractors and suppliers, and their employees.
- All potential whistleblowers and persons concerned who have a contractual relationship with the organisation should be contractually required to read and acknowledge the organisation's code of conduct and whistleblowing and whistleblower protection policy– for example, in consultancy contracts for consultants.

[19] Organisations should differentiate between the protection and support measures afforded to their personnel and other whistleblowers, where relevant.
[20] Sharing information on external whistleblowing channels shows a real commitment to facilitating the reporting of concerns and is mandatory in many countries. In EU countries, organisations are required to provide information about the procedures for reporting externally to national authorities and, where relevant, to institutions, bodies, offices or agencies of the EU.

Fostering a "speak up and listen up" culture

How potential whistleblowers – personnel and other relevant stakeholders – perceive the values expressed by their direct superiors or counterparts and an organisation's top leadership will help determine their decision to raise a concern through the IWS.

Supportive "tone from the top"

- The top leadership – the chair, board members, head of the organisation and senior management – should regularly communicate about the IWS as an organisational priority with clear, consistent and supportive messaging. Such communication should be both in writing and in person, internally to personnel, and externally to other stakeholders and the general public.
- Leadership behaviour and actions should support such communication, especially regarding leaders' commitments to integrity, protecting whistleblowers and addressing wrongdoing in the organisation.

Ethical management

- The tone from the top should trickle down through the management lines. All levels of management and all direct supervisors should express support for the IWS.
- Organisations should hold line managers accountable for their handling of whistleblower reports, especially where they are designated in the whistleblowing policy to receive these reports – for example, by including this as an aspect of their performance review.

Awards and recognitions

- Organisations should commend whistleblowers for speaking up. With their consent, they should receive public recognition from senior management – for example, via awards.

A general culture of trust, transparency and accountability

- IWS do not work in isolation, but are part of an organisation's integrity and compliance programme. Speaking up and listening up should therefore be seen as contributing to the organisation's culture of trust, transparency and accountability.

ACCOUNTABILITY TO STAKEHOLDERS THROUGH TRANSPARENCY AND PUBLIC REPORTING

Organisations should report publicly every year on their commitment to a "speak up and listen up" culture and the implementation of their IWS.

- Such reporting is a component of good governance, transparency and accountability, and can contribute to the credibility and improvement of the IWS.
- Annual reports on the functioning of the IWS and the work done to support the organisation's "speak up and listen up" culture should be communicated to its board, management, personnel and other relevant stakeholders, such as shareholders. They should also be published on the organisation's website – for example, in the section dedicated to the IWS – and included in relevant reports such as the organisation's accountability or governance report.
- The organisation's reporting should cover the following:
    - Use, outcomes and lessons learned from the IWS, including aggregated and anonymised data on the numbers of reports received; actions taken in response; outcomes, including estimated

financial damage, compensation, recoveries and sanctions; time taken to process cases and the types of wrongdoing reported. Such data is essential to show that whistleblowing reports are acted on where appropriate.[21]

- Protection of whistleblowers, including a record of the number of complaints of detrimental conduct; actions taken to follow these up and their outcomes; time taken to achieve resolution, and types of protection measures taken.
- Awareness of and trust in the IWS – for example, analysis of surveys results.

Prospective investors, partners or employees often look at whether organisations have IWS and statistics on whether these are effective. Publishing comprehensive information on the organisation's IWS in a visible and accessible way helps demonstrate that an organisation actively encourages a culture which prioritises the highest ethical standards.

[21] For guidance on how to report on use of, outcomes and lessons learned from the IWS, see Protect (2022), *Prescribed Persons – Annual Whistleblowing Reports: Best Practice Guide*. While aimed at authorities competent to receive and follow up on external whistleblowing reports, the guide includes many useful recommendations applicable to organisations reporting on their IWS.

PROCEDURES

As part of their IWS, organisations should implement systems to receive and follow up on whistleblowing reports: they must develop channels, procedures and processes.

MULTIPLE WHISTLEBLOWING CHANNELS

IWS should include multiple whistleblowing channels that are safe and easily accessible, and enable reporting in writing and orally. Organisations should recognise line managers as possible recipients of whistleblowing reports.

- Organisations should establish and operate internal whistleblowing channels in a secure manner that protects the confidentiality of the whistleblower's identity and of any third party mentioned in the report, and prevents access to that information by non-authorised personnel.
- When setting up whistleblowing channels, organisations should consider the various circumstances of potential whistleblowers and address factors such as language barriers, gender, illiteracy, disabilities, internet access and people's need to be able to submit reports within and outside regular office hours.
- Whistleblowing channels for reporting in writing should include both online options, such as email or a web-based platform, and offline options, such as post or physical "reporting boxes". Oral whistleblowing channels should include remote options, such as telephone, and physical meetings.
- At least one whistleblowing channel should enable anonymous reporting.
- IWS should provide for safe communication channels between the whistleblower and the whistleblowing officer, which allow the transfer of supporting documents. This should include a channel enabling communication with anonymous whistleblowers – for example, through an online reporting platform or an external party.

Online reporting platforms

The technical demands of setting up a secure and anonymous whistleblowing channel can seem intimidating, yet organisations do not need to develop their own system from scratch. There are a number of both open-source and proprietary providers of digital whistleblowing platforms that organisations can use.

A Transparency International U4 Helpdesk Answer provides an overview of the most common web-based whistleblower systems, exploring their respective advantages and disadvantages in terms of factors such as anonymity, security, accessibility and cost. It lays out the core principles and practical considerations for online reporting systems, as well as the chief digital threats they face and how various providers' solutions respond to

these threats. Overall, the paper has identified that open-source solutions tend to offer the greatest security for whistleblowers themselves, while the propriety software on the market places greater emphasis on usability and integrated case management functionalities.

Line managers

- Organisations should recognise line managers as possible recipients of internal whistleblowing reports, as they are the most natural and most frequently used channel for reporting work-related issues in everyday life.
- However, an IWS should highlight that while line managers have received relevant training, reporting to a line manager might not offer the same guarantees of impartiality, identity protection and effectiveness as reporting to the whistleblowing officer or office through dedicated channels.

Outsourcing reporting channels to external service providers

- If an organisation decides to outsource the operation of its reporting channels to an external provider, this should be limited to the receipt and acknowledgment of reports, and possibly the conduct of investigations (to be determined on a case-by-case basis) and the transmission of feedback from the organisation to the whistleblower. **The organisation remains in charge of following up on the report, addressing identified wrongdoing and providing feedback to the whistleblower.**
- The organisation should ensure that the external provider complies with the legal and best-practice requirements applicable to IWS, including ensuring confidentiality of the whistleblower's identity and that of other parties cited in a report, and effective communication with the whistleblower. The guarantees of independence and confidentiality should be reflected in the service contract, and in case of a breach of related obligations, this should be a shared responsibility of the external provider and the organisation.
- The role, tasks and responsibilities of the external provider should be clearly established and communicated to potential whistleblowers.

Information and advice channels

- IWS should include confidential channels where potential whistleblowers and other parties can receive comprehensive information and guidance on the scope and procedures of the IWS, the protection against detrimental conduct and remedies available, and the rights of the person concerned.
- Organisations should provide information to potential whistleblowers about available confidential, independent advice channels outside the organisation that are free of charge, such as those run by national authorities, trade unions or civil society organisations.
- Individuals seeking information and advice about whistleblowing should be fully protected, including from breaches of confidentiality and detrimental conduct.

TAKING ACTION ON WHISTLEBLOWING REPORTS

IWS should ensure diligent – that is, thorough, timely, fair and impartial – follow-up of all reports received,[22] in order to establish whether wrongdoing occurred,[23] to address confirmed wrongdoing and to correct any systemic issue identified. The follow-up of a report should involve the meaningful participation of the whistleblower.

- Organisations should develop and implement processes and procedures that ensure the follow-up of whistleblowing reports is thorough, timely, fair and impartial. The follow-up process should involve defined steps – such as initial assessment, investigation and closure – with clear criteria for taking decisions at the end of each step. IWS should provide for appeals regarding the fairness and quality of the follow-up of a report at the request of the whistleblower or the person concerned.
- Organisations should understand following up on whistleblowing reports and providing feedback to whistleblowers as obligations, and should consider failures by the person responsible to follow up on a report or to provide feedback to a whistleblower as a failure to perform duties, requiring disciplinary action as such. In some circumstances, such failures could even constitute detrimental conduct against the whistleblower.[24]
- The report follow-up should be carried out under strict confidentiality rules, on a need-to-know basis.

Communication with whistleblowers, and their participation

As knowledgeable and interested stakeholders, whistleblowers should be kept informed throughout the process and have meaningful opportunities to provide input to the follow-up on their report.

- Organisations should acknowledge receipt of a whistleblowing report within a strict, short timeframe,[25] and include information about:
    - the possibility for the whistleblower to clarify their report and provide additional information or evidence
    - the timeframe within which the whistleblower will be contacted with potential requests for clarification or further information and given feedback on the follow-up of their report
    - the whistleblower's responsibilities, such as maintaining confidentiality over the identity of the person concerned
    - the IWS – for example, sharing awareness-raising material and the organisations' whistleblowing and whistleblower protection policy.

[22] This includes anonymous reports.
[23] Or is occurring or is like to occur.
[24] In larger organisations, there should be a complaints mechanism, independent of the persons responsible for handling reports, competent to receive and follow up on reports about failures to follow up on a report or to provide feedback to a whistleblower.
[25] The EU Directive on Whistleblower Protection set the deadline at seven days.

- Communication with the whistleblower should take place regularly throughout the follow-up process. Whistleblowers should, at any time, be able to:
    - clarify their report and provide additional information or evidence – albeit without obligation to do so
    - share their concerns about risks of detrimental conduct and the protection of their identity.
- Communication with the whistleblower should include regular and timely feedback:
    - Feedback should be provided for the first time within three months of receipt of the report, and not later than completion of the assessment of the report – whichever comes first. [26]
    - Feedback should then be provided at the main steps in the follow-up process and at least every three months.
- Feedback to the whistleblower should include information on:
    - the actions envisaged or taken as follow-up to the report, the grounds for such follow-up, and the foreseen timeframe[27]
    - measures taken to protect the whistleblower's identity or anonymity; the available support and, where relevant, measures taken to protect them against detrimental conduct
    - when the whistleblower can expect further feedback on the follow-up of their report.
- Whistleblowers should be informed of the findings and outcome of the follow-up on their report. This should include information on which allegations were investigated – and if some were not, an explanation as to why; any significant limitation in the investigation;[28] conclusions reached for each allegation (whether substantiated, not substantiated or unconclusive) and an outline of corrective measures, where relevant and appropriate. Whistleblowers should be given the opportunity to review and provide comments on these results, to be included in the follow-up report.

Initial assessment of whistleblowing reports

- All reports received should be recorded, acknowledged and assessed diligently.
- Where needed, the person following up on the report should ask for further information from the whistleblower.
- At the receipt of the report and regularly throughout the follow-up process, the person handling the report should assess the risk of detrimental conduct against the whistleblower. The organisation should take measures to prevent detrimental conduct, on recommendation of the whistleblowing officer.
- More generally, at the receipt of the report and then regularly throughout the follow-up process, the person handling the report should assess risks of harm to any party, the organisation itself and the

[26] The EU Directive on Whistleblower Protection requires feedback to be provided within three months after receipt of the report was acknowledged (or after the expiry of the seven-day period after the report was made, if no acknowledgment was sent), but does not require further feedback at a later stage. However, providing feedback to the whistleblower only once is not sufficient.
[27] When the organisation can only provide limited feedback to a whistleblower, the reasons for such limited details should be clearly explained (e.g. the organisation's duties of confidentiality to other personnel, or other legal limitations).
[28] For example, there could be limitations in who can be interviewed to obtain statements or correlate facts if a person is no longer affiliated with the organisation, has left a country or refuses to collaborate.

public interest. The organisation should take support and protection measures, on recommendation of the whistleblowing officer.

- In organisations receiving large numbers of reports, it might be necessary to prioritise further treatment of reports based on risk, such as risk of harm to the individual, the public interest or the organisation, while ensuring timely follow-up of all reports received.
- Where a report is found to be beyond the scope of the IWS, the whistleblower should be directed to another internal reporting or complaint system, where available. Reports with mixed or unclear scope received through internal whistleblowing channels should be managed through the IWS, in coordination with other internal reporting systems, where appropriate.

Investigation of reported wrongdoing

- The person following up on the report should be able to carry out or oversee the investigation with sufficient independence from the whistleblower, the person concerned and other interested parties.
- Investigations should follow due process. Where a person is suspected of wrongdoing (such as the person concerned), that person should be presumed innocent and have the right to respond and to receive assistance. However, the investigator should not provide information which may disclose the identity of the whistleblower.
- For each investigation, the person responsible for handling the case should develop clear terms of reference, identifying the scope, methods and skills required. Investigations should be properly resourced, and the persons involved in carrying out the investigation, both internal and external, should have the required competencies.
- Investigations should observe "victim/survivor-focused" principles when appropriate, such as in cases of bullying, sexual harassment, sextortion or sexual exploitation, and should be conducted in a way that avoids re-traumatisation and prioritises the wellbeing, needs and wishes of the victims.
- Organisations should consider adopting investigation protocols.
- The investigation result should be considered preliminary until presented to the whistleblower for their review and potential comments, to be included in the investigation report.

Closure of follow-up

- A case is closed when a conclusion has been reached and no additional information with the potential to change the outcome is presented. Where necessary – for example, if the whistleblower brings new material arguments or evidence – the investigation should be re-opened.
- If the investigation found that wrongdoing is occurring, has occurred or is likely to occur, organisations should take necessary action to address it. This should include, as appropriate, measures to:
    - stop or prevent the wrongdoing
    - sanction the author(s) of the wrongdoing where they have been identified
    - remedy any damage caused
    - report to the competent authorities.
- Organisations should take appropriate action to correct any systemic issue identified, such as weaknesses in policy or procedure, whether or not wrongdoing could be established, to ensure that it does not occur in the future or recur, and lead to more serious harm.

- Organisations should take measures to protect the whistleblower and their identity beyond the closure of the case.

RECORD-KEEPING AND DATA PROTECTION

Reports received, actions taken as follow-up, and the findings and outcome of the follow-up, as well as communication with the whistleblower and concerned person, should be adequately documented and kept in retrievable and auditable form in accordance with confidentiality and data protection requirements.

- Organisations should keep records of every report received, in compliance with confidentiality requirements. Reports should be stored for no longer than necessary and proportionate to comply with legal requirements, which include the diligent follow-up of whistleblowing reports and the protection of whistleblowers against detrimental conduct.
- Organisations should have systems to record the number of whistleblowing reports received, the corresponding actions taken in response and their outcomes – including the estimated financial damage, compensation, recoveries and sanctions. They should also record the time taken to follow up on reports and the types of wrongdoing reported, with data subsequently shared in aggregated and anonymised form with the board, personnel and other relevant stakeholders, such as shareholders and the general public.[29]

Record keeping of oral reports under the EU Directive

Organisations have an obligation to ensure, subject to the consent of the whistleblower, complete and accurate records of oral reports in a durable and retrievable form.

- Oral reports made through a recorded telephone line or another recorded voice messaging system can be documented by organisations via either a recording of the conversation or as a complete and accurate transcript, prepared by the person handling the report.[30]
- Oral reports made through an unrecorded telephone can be documented by organisations in the form of accurate minutes of the conversation written by the person handling the report.
- Oral reports made through an in-person meeting can be documented by organisations via a recording of the conversation or accurate minutes of the meeting, prepared by the person handling the report.
- For all oral reports, organisations should offer the whistleblower the opportunity to check, rectify and agree, by signing, documentation of the report made via transcript or minutes of a conversation or meeting.

In essence, implementing IWS involves processing personal data – for example, about the whistleblower, the person concerned and witnesses.

[29] Larger organisations should consider adopting some form of case-management system for the recording, follow-up and monitoring of reports. Such a system enables organisations to collect and review key statistics about reports on a regular basis and makes it easy to give feedback to whistleblowers about the status of their report.
[30] Organisations should obtain the whistleblowers' consent before audio recording of the phone conversation or the voice message begins.

- The design and implementation of the IWS should include a consultation with the organisation's internal data protection officer, if one is nominated, or alternatively the relevant data protection authorities in the country, if they exist.
- Organisations should provide information to potential whistleblowers about how their data will be processed, how long it will be retained and for what purpose.
- Personal data which is manifestly not relevant for the handling of a specific report should not be collected or, if collected, should be deleted without undue delay.

IWS and the EU General Data Protection Regulation (GDPR)

Organisations in the EU need to ensure that their IWS meet the technical and organisational requirements of the GDPR. These include:

- Organisations should clearly identify the purpose of the IWS.
- Organisations should be able to demonstrate that they have assessed and mitigated privacy risks at the design and implementation stages of the IWS. Some organisations may also have a duty in certain countries to submit their data protection impact assessment to the relevant data protection authorities.
- The IWS should apply the principle of data minimisation, and only process personal information that is adequate, relevant and necessary for handling a case.
- The IWS should define proportionate conservation periods for the personal information processed for the handling of a whistleblowing report, depending on the follow-up outcome. For example, reports found to be beyond the scope of the IWS at the end of the initial assessment stage should not be kept for as long as reports where an investigation has been launched.
- The persons involved in a whistleblowing report – the whistleblower, the person concerned and other third parties mentioned in the report – should be informed about the way their personal data will be processed as soon as practically possible. In cases where informing the person concerned at an early stage may jeopardise the investigation of a report, the sharing of specific information with that person may be deferred. The decision to defer information should be made on a case-by-case basis and the reasons documented.
- If organisations outsource part of the processing of whistleblowing cases – for example, whistleblowing channels or investigations – they should have a personal data processor agreement in place.

Source: European Data Protection Supervisor (2016), *Guidelines on processing personal information within a whistleblowing procedure,* https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en

SUPPORT AND PROTECTION FOR WHISTLEBLOWERS

A variety of measures is necessary to ensure effective protection of whistleblowers and other parties at risk, including protecting their identity; prohibiting, preventing and addressing detrimental conduct, and providing support.

When establishing their IWS, organisations should consider how to provide protection and support to all categories of potential whistleblowers and protected parties. This includes the categories of persons able to report through the organisation's internal whistleblowing channels and the categories of persons afforded protection by law. These do not always align.[31]

PROTECTING THE IDENTITY OF WHISTLEBLOWERS AND OTHER PROTECTED PERSONS

One of the most effective ways of protecting a whistleblower against detrimental conduct is to protect their identity. There are two different ways to protect the identity of a whistleblower: preserving confidentiality and allowing anonymous reporting. The IWS should explain the difference between confidentiality and anonymity.

Confidentiality

Without the explicit consent of the whistleblower, their identity and any identifying information – that is, information from which the identity of the whistleblower may be directly or indirectly deduced – should not be disclosed beyond those persons competent to receive or follow up on reports.

- Organisations should establish and operate their IWS in a secure manner that ensures confidentiality of the whistleblower's identity and that of any third party mentioned in the report, and prevents access to that information by non-authorised personnel.
- All persons competent to receive or follow up on whistleblower reports should be bound by the same duty of confidentiality.
- The whistleblower's identity may only be disclosed where there is a legal obligation to do so. Organisations should provide potential whistleblowers with clear information about these exceptions to

[31] For example, while most whistleblower protection laws do not protect "outsider" whistleblowers, such as users, customers or beneficiaries, an organisation might have decided to enable them to report through its IWS. Conversely, much legislation, including the EU Directive, only requires organisations to enable their own workers to report through internal whistleblowing channels, but extends whistleblower protection to any person who reported information acquired in the context of their work-related activities.

confidentiality, via channels such as policies and training, and should further communicate them to actual whistleblowers.

- When identifying information must be disclosed, organisations should inform the whistleblower beforehand with sufficient notice, via a written explanation,[32] and should provide them with additional protection measures where appropriate. The whistleblower should have the opportunity to appeal the decision to disclose their identity.
- The IWS should explain to potential whistleblowers that the protection offered by confidentiality is not absolute in practice. For example, if the organisation is very small, or if before making a report the whistleblower has mentioned their concerns to colleagues, there is a risk that the report will be traced back to them.
- Organisations should establish effective, proportionate and dissuasive penalties for breaching the duty of confidentiality over a whistleblower's identity.

Anonymity

Organisations should accept and follow up on anonymous reports, and protect anonymous whistleblowers.

- At least one internal whistleblowing channel should enable anonymous reporting.
- A safe channel should enable communication between anonymous whistleblowers and the person handling their report – for example, through an online reporting platform or an external party.
- The IWS should explain to potential whistleblowers that the protection offered by anonymity is not absolute, highlighting practical issues, for example:
    - If the organisation is very small, or if before making a report the whistleblower has mentioned their concerns to colleagues, there is a risk that the report will be traced back to them.
    - As anonymity means the person handling the case does not know who they are protecting, it can be more difficult for them to prevent the whistleblower's identity from being discovered.
- Regardless of whether an organisation itself receives and follows up on anonymous reports, it should protect whistleblowers who report information on wrongdoing anonymously – internally, externally or via public disclosure – and are subsequently identified.

The benefits of accepting and following up on anonymous reports

- Welcoming anonymous reports helps build trust in the IWS:

  - It tells potential whistleblowers and other stakeholders that addressing wrongdoing is more important than identifying who is blowing the whistle.

[32] The EU Directive on Whistleblower Protection foresees an exception when such information would jeopardise the related investigations or judicial proceedings.

- It encourages people to speak up by enabling individuals who would not otherwise do so for fear of negative consequences or that insufficient care will be taken to protect their identity.[33]

- Anonymous reports can provide valuable information about wrongdoing that puts the organisation or the public interest at risk:

  - The overall substantiation rate for anonymous reports is lower than reports from whistleblowers who identify themselves, but it is still comparable.[34] It can be improved with the use of communication channels that enable exchanges between anonymous whistleblowers and the persons handling their report.

  - Trivial or false reports are uncommon, including when anonymous reports are allowed.[35]

- In practice, anonymous whistleblowers often reveal their identity after a few exchanges with the person handling their report.

PROTECTION FROM DETRIMENTAL CONDUCT AND INTERFERENCE

What is detrimental conduct?

Detrimental conduct is any threatened, recommended or actual, direct or indirect act or omission linked to or resulting from actual or suspected whistleblowing, which causes or may cause harm – for example, physical or psychological harm, damage to the person's reputation, financial loss, or pain and suffering. Detrimental conduct can be intentional or can result from an organisation's failure to support and protect a whistleblower.

It includes, for example:

- suspension, dismissal or equivalent measures
- failure to convert a temporary employment contract into a permanent one[36]
- failure to renew, or early termination of, a temporary employment contract
- constructive discharge (quitting when an organisation makes working conditions intolerable)
- demotion or withholding of promotion
- transfer of duties, reduction or limitation of work assignments, change in working hours
- unfair selection for tasks or attendance at events, withholding of training
- restrictions on or removal of available resources, such as budgets or human resources
- reduction in remuneration or withholding of payment
- negative performance assessment or employment reference

[33] For example, a 2015 survey of French employees found that 20 per cent of workers would blow the whistle only anonymously (Harris Interactive, "*Lanceurs d'alerte": quelle perception de la part des salariés*? 2015, p.9)
[34] For example, Navex, which provides reporting management systems to thousands of organisations across the globe, found a substantiation rate of 50 per cent for reports by named whistleblowers and of 39 per cent for anonymous reports (Navex, 2022 Risk & Compliance Hotline & Incident Management Benchmark Report).
[35]For example, in a survey of European companies, 78 per cent of respondents stated that the share of abusive reports is below 2 per cent, with 43 per cent stating that the value is below 1 per cent (EQS Group, Analyses and statistics about whistleblowing systems in Europe, 2021).
[36] This is in cases where the worker had legitimate expectations that they would be offered permanent employment.

- unwarranted inspection or investigation of duties, or disclosure of the result of such inspections
- imposition or administering of any disciplinary measure, reprimand or other penalty
- coercion, intimidation, harassment or ostracism
- discrimination, or disadvantageous or unfair treatment
- boycotting or blacklisting
- early termination or cancellation of a contract for goods or services
- disclosure of the whistleblower's identity
- prosecution or legal action
- physical or psychological violence
- smearing, discrediting or humiliating of a person by questioning their mental health, professional competence, reliability or honesty.

Prohibition of detrimental conduct and interference

Organisations should prohibit any form of detrimental conduct linked to whistleblowing, and any interference with whistleblowing.

- Organisations should broadly define detrimental conduct to include any act or omission which causes or may cause harm to the whistleblower or other protected parties (see box above). Any list an organisation provides defining forms of detrimental conduct should be indicative and non-exhaustive, and include forms of detrimental conduct specific to whistleblowers who are not employees, such as blacklisting, early termination of a contract for goods or services, or cancellation of a licence or permit.
- Both the code of conduct or ethics and the whistleblowing policy should clearly prohibit:
    - any form of detrimental conduct against whistleblowers and protected third parties, including threats of detrimental conduct and attempts at such conduct, such as seeking to identify a whistleblower.
    - hindering or attempting to hinder whistleblowing (interference with whistleblowing).
- Organisations should provide for sanctions for detrimental conduct linked to whistleblowing, and for interference with whistleblowing.

Preventing detrimental conduct

Organisations should take reasonable steps to prevent detrimental conduct and to ensure that individuals and entities under their control or working for them refrain from detrimental conduct.

- Organisations should expressly commit not to enter into agreements that might waive or obstruct a whistleblower's rights and protections, including pre-dispute arbitration agreements, loyalty clauses in contracts, or confidentiality or non-disclosure agreements. This can be achieved by including in such agreements and in organisational policies and procedures clauses explicitly recognising the

whistleblower rights and protections afforded by the organisation's IWS, and stating that in the event of a conflict or perceived conflict with the whistleblowing policy, the whistleblowing policy shall prevail.

- Organisations should ensure that persons and entities working directly or indirectly for the organisation, and under any form of contract or agreement with it, are aware that detrimental conduct against whistleblowers and other protected persons is prohibited by its code of conduct and whistleblowing policy, and that it will sanction detrimental conduct (see the information and communication section for detailed recommendations on means). Such persons and entities include current and former employees, executive personnel, board members, interns, student workers, volunteers, contractors, sub-contractors, suppliers or consultants.
- Organisations should implement strategies to prevent detrimental conduct against whistleblowers throughout the follow-up process and after the conclusion of the case, such as systematic and regular risk assessments and preventive measures.
- Organisations should take measures to prevent risks of further harm to the whistleblower pending the resolution of an internal detrimental conduct complaint, for example, suspending disciplinary processes or providing paid leave.[37]
- Failure by the person responsible to take reasonable steps to prevent detrimental conduct should be considered a failure of duty and be disciplined as such. In some circumstances, such failure could even constitute detrimental conduct against the whistleblower.[38]

ADDRESSING DETRIMENTAL CONDUCT, INTERFERENCE AND BREACHES OF CONFIDENTIALITY

IWS should provide for enforceable, transparent and timely mechanisms to (1) receive and follow up on complaints of detrimental conduct, interference and breach of confidentiality, (2) sanction perpetrators and (3) ensure full reparation of affected whistleblowers and other protected persons, providing for remedial measures and compensation.[39]

- Organisation should provide enforceable, transparent and timely mechanisms to receive and follow up on complaints about:
    - detrimental conduct against whistleblowers and protected third parties
    - hinderance or attempts to hinder whistleblowing (interference)
    - breaches of confidentiality over the whistleblower's identity.
- Once it is established that an individual complaining about detrimental conduct is a whistleblower or another protected person, and that they have suffered detriment, it should fall on the person who is responsible for the detrimental conduct to clearly and convincingly demonstrate that it was not linked in any way to actual or suspected whistleblowing.
- If the occurrence of detrimental conduct is confirmed, the organisation should take necessary action to:

[37] Once it is established that the individual complaining about detrimental conduct had made an internal or external report, or a public disclosure, and suffered detriment.
[38] In larger organisations, there should be a complaint mechanism, independent of the persons responsible for handling reports, competent to receive and follow up on reports about failures to follow up on a report or to provide feedback to a whistleblower.
[39] Such mechanisms should be part of the IWS, and not the grievance system or other systems, to maintain confidentiality over the whistleblower's identity.

- stop the detrimental conduct
- protect the physical, financial and psychological wellbeing of the person suffering detrimental conduct
- remedy any loss, including indirect and future losses and financial and non-financial losses. To the greatest extent possible, the whistleblower should be restored to a situation they were in – or would have been in – had they not suffered detrimental conduct.

Examples of restorative actions:

- reinstatement of the person either to the position they occupied before detrimental conduct or to a similar position with equal salary, status, duties and working conditions
- fair access to any promotion and training that may have been withheld
- restoration of duties, if possible
- recognition of lost time and impact on performance
- withdrawal of litigation against a whistleblower
- deletion of any records that could constitute a dossier for blacklisting or later retaliation
- relaunching a procurement process
- restoration of a cancelled contract
- apologies for failures
- commendation for upholding the organisation's mission, values or interest through speaking up about wrongdoing – for example, a Speak Up Award
- financial compensation for past, present and future lost earnings
- financial compensation for pain and suffering, including medical expenses.

Holding the perpetrators of detrimental conduct, interference and breach of confidentiality accountable

- Organisations should provide for effective, proportionate and dissuasive penalties for:[40]
  - detrimental conduct against whistleblowers and protected third parties
  - hindering or attempting to hinder whistleblowing (interference)
  - breaching confidentiality of the whistleblower's identity.
- Detrimental conduct, interference or breach of confidentiality over a whistleblower's identity committed by the organisation's employees should be considered serious or gross misconduct. When such misconduct is established, it should trigger the initiation of formal disciplinary proceedings against the perpetrator.

[40] Effectiveness requires that a penalty is capable of achieving the desired goal, i.e. observance of the rules. Proportionality requires that a penalty is commensurate with the gravity of the wrongdoing and its effects, and does not exceed what is necessary to achieve the desired goal. Dissuasiveness requires that a penalty has a deterrent effect on the wrongdoer, preventing them from repeating the wrongdoing, and on other potential wrongdoers.

- Organisations should establish procedures and appropriate penalties to sanction detrimental conduct by persons others than employees, who are not subject disciplinary procedures, such as consultants, suppliers, board members and volunteers. Sanctions could include, for example, removal from a position and termination or non-completion of a contract. Such situations should be foreseen in the organisation's contractual arrangements with external parties.
- Where the detrimental conduct constitutes a violation of the law, organisations should report it to the competent authorities and consider pursuing civil, criminal or administrative legal action through the relevant authorities.
- Organisations should apply sanctions consistently and openly to show their commitment to their whistleblower protection policy and to deter those who might consider detrimental conduct against whistleblowers.[41]
- Those accused of detrimental conduct, interference or breach of confidentiality should have the right to respond and to receive assistance.

SUPPORTING WHISTLEBLOWERS

Organisations should provide support to whistleblowers to prevent harm to their health or career.

Whistleblowing often causes stress or even fear, and is time-consuming. It can therefore impact negatively on a whistleblower's performance and health, resulting in damage to their career and potential financial losses. Organisations should provide support to whistleblowers to prevent or minimise such harm. This includes:

- offering support measures, such as an alternative line manager or workspace, access to psychological support services and confidential counselling
- ensuring that the persons responsible for receiving reports and communicating with the whistleblower – such as the whistleblowing officer, line managers or an external service provider – are trained in how to listen and create psychological safety.

[41] Organisations should openly report aggregated data on the number and types of sanctions taken for detrimental conduct; failure to take reasonable steps to prevent detrimental conduct; interference with whistleblowing; and breaches of confidentiality over whistleblower identity (see section on information and communication).

PROTECTION OF THE PERSON CONCERNED

The person(s) referred to in a whistleblower's report as responsible for the suspected wrongdoing should also benefit from protection measures.

Organisations should protect the identity and the rights of the person concerned, including by providing for effective, proportionate and dissuasive sanctions for individuals who knowingly report false information.

The person concerned is the person referred to in a whistleblowing report as a person responsible for the suspected wrongdoing or detrimental conduct, or associated with that person. It can be a natural or a legal person.

- The identity of the person concerned should be protected.
- The person concerned should be presumed innocent, and have the right to respond and to receive assistance during the follow-up of a report, in accordance with the requirement to protect the identity of the whistleblower.
- Organisations should provide for effective, proportionate and dissuasive sanctions for individuals who knowingly report false information.
    - Organisations should refrain from using words such as "malicious" or "abusive" when referring to knowingly false reporting.[42]
    - The burden to prove that the whistleblower knew the information was false at the time of reporting should fall on the person making that claim.

[42] Use of the terms "abusive" and "malicious" might suggest that the whistleblower's motives for making a report will be examined to determine whether or not they will be protected, whereas best practice dictates that organisations should protect whistleblowers without any consideration of their motives for reporting.

CONTINUOUS MONITORING AND REVIEW

IWS should be continuously monitored and regularly reviewed and revised.

IWS should be formally reviewed at least annually, and revisions should be made accordingly to improve effectiveness and ensure systems are up to date and in line with legislation and best practice.

- Organisations should develop indicators to monitor implementation and assess the effectiveness and suitability of the IWS.
- Reviews can be conducted internally, but IWS should also undergo regular independent external reviews, either by state authorities or professional advisors or civil society organisations commissioned by the organisation.
- Reviews should involve relevant stakeholders, including employees, trade unions or other personnel representatives.
- An organisation's board should receive regular reports from the whistleblowing officer or office and the head of the organisation on the results of reviews, and make independent assessments of IWS adequacy.
- Organisations should publicly report on the reviews' main findings and outcomes.

Reviews of the IWS should answer, inter alia, the following questions:

- One year after the entry into force of your system, has your organisation allocated human and financial resources to allow the effective operation of the system?
- Has your organisation created a specific department for its ethics or compliance policy and IWS? If not, to which department did it attach the whistleblowing officer or office?
- Is the average time taken to follow up on a report and provide feedback to the whistleblower less than or equal to three months?
- Have you planned and carried out audits, internal and/or external, of the IWS? How regularly? With what results?
- Are audits of the system carried out by the board of directors?
- Has your IWS been reviewed by a competent authority, such as an anti-corruption agency or whistleblowing authority? With what results?

- In the past year, have you conducted awareness training or other awareness activities regarding the IWS for all potential whistleblowers?
- In the past year, have you conducted a survey measuring personnel awareness and trust in the IWS? What were the results?
- In the past year, have you received any reports? How many?
- In the past year, have you received any complaints of detrimental conduct? How many?
- In the past year, have any reports been followed up? How many?
- In the past year, have any whistleblowing reports or complaints of detrimental conduct resulted in disciplinary action or prosecution? How many?
- Do you have a systematic follow-up procedure to ensure whistleblowers do not suffer reprisals over time – for example, after three months, six months, a year and two years?
- Does the whistleblowing officer or office produce an annual report with anonymised data? Who is it shared with and what is its use?
- Is your IWS inclusive and gender-sensitive? Do you collect and analyse disaggregated data to identify and address gendered patterns of reporting and barriers to reporting, including detrimental conduct, considering both gender and other factors that shape individual experiences of reporting, such as race, ethnicity or disability?
- Do you have a mechanism in place to revise your IWS following audits and annual reports? What is the timeline?

REFERENCES AND RESOURCES

RESOURCES FROM TRANSPARENCY INTERNATIONAL

Andy McDevitt and Marie Terracol (2020), *Assessing Whistleblowing Legislation: Methodology and Guidelines for Assessment Against the EU Directive and Best Practice,* Transparency International, www.transparency.org/en/publications/assessing-whistleblowing-legislation

Jacqueline de Gramont (2017), *The Business Case for "Speaking Up": How Internal Reporting Mechanisms Strengthen Private-Sector Organisations*, Transparency International, www.transparency.org/en/publications/business-case-for-speaking-up

Marie Terracol (2019), "Building on the EU Directive on Whistleblower Protection", Position Paper, Transparency International, www.transparency.org/whatwedo/publication/building_on_the_eu_directive_for_whistleblower_protection

Marie Terracol (2018), *A Best Practice Guide for Whistleblowing Legislation,* Transparency International, www.transparency.org/whatwedo/publication/best_practice_guide_for_whistleblowing_legislation

Transparency International (2013), International Principles for Whistleblowing Legislation, www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation

Peter Wilkinson (2017), *10 Anti-Corruption Principles for State-Owned Enterprises*, Transparency International, www.transparency.org/en/publications/10-anti-corruption-principles-for-state-owned-enterprises

Marie Chêne (2021), "Finding a voice, Seeking Justice – the barriers women face to reporting corruption in the European Union", Position Paper, Transparency International, www.transparency.org/en/publications/finding-voice-seeking-justice-barriers-women-face-reporting-corruption-european-union

Transparency International Ireland (2021), *National Integrity Index 2021, Public-Sector Bodies (Part 1), Semi-States and Universities*, www.transparency.ie/resources/national-integrity-index/semi-state-universities-index-2021/report

Dr Roland Gjoni (2021), *National Integrity Index 2020, Private Sector: Assessing Disclosure Practices of 30 Irish Companies*, Transparency International Ireland, www.transparency.ie/resources/national-integrity-index/private-sector-index/report-2020

Transparency International Helpdesk Answers

Matthew Jenkins (2020), "Overview of whistleblowing software", U4 Helpdesk Answer, Transparency International, https://knowledgehub.transparency.org/helpdesk/overview-of-whistleblowing-software

Nieves Zúñiga (2020), "Gender Sensitivity in Corruption Reporting and Whistleblowing", U4 Helpdesk Answer, Transparency International, https://knowledgehub.transparency.org/helpdesk/gender-sensitivity-in-corruption-reporting-and-whistleblowing

Kaunain Rahman (2018), "The impact of General Data Protection Regulation on whistleblowing", Transparency International, https://knowledgehub.transparency.org/helpdesk/the-impact-of-the-general-data-protection-regulation-on-whistleblowing

Caitlin Maslen (2018), "Financial incentives for whistleblowers", Transparency International, https://knowledgehub.transparency.org/helpdesk/financial-incentives-for-whistleblowers

Suzanna Khoshabi (2017), "Internal Whistleblowing Mechanisms", Topic Guide, Transparency International, https://knowledgehub.transparency.org/guide/topic-guide-whistleblowing/4250

OTHER RESOURCES

International Chamber of Commerce (2022), Guideline on Whistleblowing, https://iccwbo.org/publication/icc-2022-guidelines-on-whistleblowing/

International Organization for Standardization (ISO) (2021), Whistleblowing management systems — Guidelines,, ISO 37002:2021

UNODC (2021), Speak Up for Health! Guidelines to enable whistle-blower protection in the health-care sector, www.unodc.org/documents/corruption/Publications/2021/Speak_up_for_Health_-_Guidelines_to_Enable_Whistle-Blower_Protection_in_the_Health-Care_Sector_EN.pdf

OECD (2021), *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, OECD/LEGAL/0378, www.oecd.org/corruption/2021-oecd-anti-bribery-recommendation.htm

Vigjilenca Abazi (2021), Guide to Internal Whistleblowing Channels and the Role of Trade Unions, Eurocadres, www.eurocadres.eu/publications/guide-internal-whistleblowing-channels-and-the-role-of-trade-unions

Kai-D Bussmann, Sebastian Oelrich, Andreas Schroth, Nicole Selzer (2021), *The Impact of Corporate Culture and CMS: A Cross-Cultural Analysis on Internal and External Preventive Effects on Corruption*

European Parliament and Council of the European Union (2019). *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

European Data Protection Supervisor (2016), Guidelines on processing personal information within a whistleblowing procedure, https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en

Protect (2022), *Prescribed Persons – Annual Whistleblowing Reports: Best Practice Guide, https://public-concern-at-work.s3.eu-west-1.amazonaws.com/wp-content/uploads/images/2022/08/30095958/Annual-Whistleblowing-Reports-Best-Practice-Guide.pdf*

CREATE CHANGE WITH US

ENGAGE

Follow us, share your views and discuss corruption with people from around the world on social media.

facebook.com/TransparencyInternational/
twitter.com/antikorruption/
linkedin.com/company/transparency-international/
instagram.com/Transparency_International/
youtube.com/user/TransparencyIntl/

LEARN

Visit our website to learn more about our work in more than 100 countries and sign up for the latest news in the fight against corruption.

transparency.org

DONATE

Your donation will help us provide support to thousands of victims of corruption, develop new tools and research and hold governments and businesses to their promises. We want to build a fairer, more just world. With your help, we can.

transparency.org/donate

Transparency International
International Secretariat
Alt-Moabit 96, 10559 Berlin, Germany

Phone: +49 30 34 38 200
Fax: +49 30 34 70 39 12

ti@transparency.org
www.transparency.org

Blog: transparency.org/en/blog
Facebook: /transparencyinternational
Twitter: @anticorruption