UNODC
United Nations Office on Drugs and Crime

SPEAK UP FOR HEALTH!

GUIDELINES TO ENABLE WHISTLE-BLOWER PROTECTION IN THE HEALTH-CARE SECTOR

UNITED NATIONS OFFICE ON DRUGS AND CRIME

SPEAK UP FOR HEALTH!

GUIDELINES TO ENABLE WHISTLE-BLOWER PROTECTION IN THE HEALTH-CARE SECTOR

UNITED NATIONS
Vienna, 2021

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

CONTENTS

ACKNOWLEDGEMENTS

These guidelines were produced by the United Nations Office on Drugs and Crime (UNODC). They were developed with generous funding from the Foreign, Commonwealth and Development Office of the United Kingdom of Great Britain and Northern Ireland and the Bureau of International Narcotics and Law Enforcement Affairs of the United States of America.

UNODC acknowledges with profound gratitude all those who have contributed their expertise and experience to the development of these guidelines.

UNODC would especially like to thank the experts who participated in the expert group process, which included a virtual meeting held on 25 January 2021, and those who provided written and oral feedback: Juha Keränen, Ministerial Adviser, Ministry of Finance of Finland; Martin Fletcher, Chief Executive Officer, Australian Health Practitioner Regulation Agency, and Adjunct Professor, Royal Melbourne Institute of Technology (RMIT University); May Giuliani, Corporate Counsel, Australian Health Practitioner Regulation Agency; Aled Jones, Professor of Patient Safety and Healthcare Quality, School of Healthcare Sciences, Cardiff University; Brian Mdlalose, State Advocate, National Prosecuting Agency of South Africa; Cherese Thakur, Advocacy Coordinator, amaBhungane Centre for Investigative Journalism, South Africa; Georgia Georgiadou, Deputy Head of Unit, European Commission; Maria Mollica, Policy Officer, European Commission; Khadija Sharife, Investigative Journalist, Coordinator of the Platform to Protect Whistleblowers in Africa, South Africa; Gabriella Razzano, Director, OpenUp, South Africa; Helené Donnelly OBE, Ambassador for Cultural Change and Lead Freedom to Speak Up Guardian, Staffordshire and Stoke on Trent Partnership National Health Service (NHS) Trust; Leonie Raby, Senior Intelligence Adviser National Guardian's Office, United Kingdom; and Sam Bereket, Intelligence and Case Review Manager, National Guardian's Office, United Kingdom.

UNODC also wishes to thank the experts Sheryl Goodman, President, Procurement Integrity Consulting Services, and Ashley Savage, a specialist in whistle-blowing, information rights and governance, as well as UNODC consultants Suhaas Ema and Alberto Martínez García, for their substantive contribution to the drafting of these guidelines.

The guidelines benefited from the valuable input of UNODC staff members who reviewed and commented on various sections of this guide, including the following: Giovanni Gallo, Julia Pilgrim, Louise Portas, Kari Rotkin, Jennifer Sarvary-Bradford, Tim Steele and Brigitte Strobel-Shaw from the Corruption and Economic Crime Branch.

GLOSSARY

Health-care sector: a collective group of all legal or natural persons involved in providing and coordinating medical and related goods and services.

Health-care sector organization: any entity, whether public or private, that provides or coordinates the provision of medical or related goods and services. This term can also be used to refer to a health-care sector facility, defined as any facility, whether public or private, that provides medical or related goods and services, including, but not limited to, military hospitals, mental health units and prison medical wards.

Internal investigation: an examination of reports conducted within an organization, with the aim of establishing facts.

Investigator or fact-finder: a person responsible for carrying out an internal investigation of reported wrongdoing or retaliation within the organization. The fact-finder is also in charge of drafting the final report and recommending further action to be taken after the investigation has concluded.

Initial recipient of report: a person in charge of receiving a disclosure made by a reporting person and, in most cases, of handling the initial assessment of a report.

Report: the disclosure of an irregularity that has occurred, is occurring or is likely to occur within an organization.

Reportable wrongdoing: an instance of a work-related misconduct or wrongdoing, including an omission, that corresponds to the level of gravity established in the organization's whistle-blower protection policy.

Reporting channel: a system established to disclose alleged wrongdoing and irregularities in a safe manner and designed to minimize the risk of retaliation.

Reporting interface: a means by which a reporting person makes a report through a reporting mechanism. Examples of reporting interfaces: face-to-face, telephone, email, online and digital applications, among others.

Reporting person: an individual who discloses a reportable wrongdoing in the workplace.

Retaliation: unfair or unjustified treatment suffered by a whistle-blower as a consequence of a report previously made.

Whistle-blower: a reporting person, falling within the categories of defined persons able to report according to the organization's whistle-blower protection policy, who discloses a reportable wrongdoing in good faith and/or on reasonable grounds using the established reporting channels.

EXECUTIVE SUMMARY

CORRUPTION: AN ENDEMIC PROBLEM IN THE HEALTH-CARE SECTOR

The health-care sector is broad, complex and vulnerable to corruption.[1] The sector's vulnerabilities include the complexities of national health-care systems, the wide range of activities along the entire medical supply chain and the large number of actors, often from both the public and the private sectors. In addition, the vast quantities of assets involved make the sector particularly susceptible to corruption.[2] These vulnerabilities can also weaken health-care systems, waste resources and make countries less resilient to – and less agile in – health emergencies, compromising coverage and access to essential health-care services.[3] A lack of safeguards and controls in the medical product supply chain can result in the purchase and distribution of low quality, expired or even falsified products and drugs.[4] Corruption enables the production, purchase and use of falsified medical products.[5] At best, such medical products are inefficient; at worst, they harm consumers. In both cases, they endanger the lives of the people who need them the most.

The estimated cost of corruption in the health-care sector is already very high under normal circumstances. For instance, in 2008, the World Health Organization (WHO) estimated that out of $5.7 trillion spent worldwide on health, $415 billion (around 7.3 per cent) was lost to health-related fraud and abuse.[6]

The risk of corruption in the health-care sector becomes even greater and its devastating effects become more evident in times of health and sanitary crises.

REPORTING CORRUPTION IN THE HEALTH-CARE SECTOR: A CRITICAL STEP TO ADDRESS OFFENCES AND SAVE LIVES

Preventing corruption in the health-care sector is critical because of the undue risk it poses to human lives. It is essential, therefore, that States and health-care sector organizations establish safeguards and oversight mechanisms to prevent corruption.[7]

However, despite all the preventive measures that may be established, corruption or other serious wrongdoing can still occur. It is therefore critical that health-care sector organizations establish mechanisms to detect wrongdoing and address it at the earliest stage possible.

[1] Tim K. Mackey, Taryn Vian and Jillian Kohler, "The sustainable development goals as a framework to combat health-sector corruption", *Bulletin of the World Health Organization*, vol. 96, No. 9 (September 2018), pp. 634–643.

[2] See, for instance, Oslo statement on corruption involving vast quantities of assets, in particular recommendation 8, in United Nations Office on Drugs and Crime (UNODC), "Preventing and combating corruption involving vast quantities of assets: expert recommendations" (Vienna, 2019).

[3] Mackey, Vian and Kohler, "The sustainable development goals as a framework to combat health-sector corruption", *Bulletin of the World Health Organization*, vol. 96, No. 9 (September 2018), pp. 589–664.

[4] UNODC, Research and Trend Analysis Branch, "Report on the COVID-19-related trafficking of medical products as a threat to public health", research brief (Vienna, 2020).

[5] UNODC, *Combating Falsified Medical Product-related Crime: A Guide to Good Legislative Practices* (Vienna, 2019).

[6] Ben Jones and Amy Jing, "Prevention not cure in tackling health-care fraud", *Bulletin of the World Health Organization*, vol. 89, No. 12 (December 2011), pp. 858–859.

[7] UNODC, "Accountability and the prevention of corruption in the allocation and distribution of emergency economic rescue packages in the context and aftermath of the COVID-19 pandemic", policy document (Vienna, 2020).

One such mechanism is aimed at encouraging personnel in health-care organizations to report suspected wrongdoing and protecting them from retaliation in any form.

In this regard, under article 33 of the United Nations Convention against Corruption, States parties are required to consider incorporating into their domestic legal systems appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with the Convention. States parties are also required, under article 8, paragraph 4, to consider establishing measures and systems to facilitate the reporting by public officials of acts of corruption to appropriate authorities, when such acts come to their notice in the performance of their functions.

Establishing an effective reporting system and a corresponding whistle-blower protection mechanism is thus recognized as one of the strongest measures for detecting wrongdoing at an early stage[8] and enabling the rapid implementation of mitigation measures that may prevent the reported wrongdoing from becoming a large-scale corruption case or causing harm to patients. In the health-care sector, establishing such a reporting mechanism can therefore prevent harm and save lives.

The present guidelines provide a step-by-step process that an organization can follow to establish internal policies and procedures that facilitate the disclosure of allegations of wrongdoing and protect reporting persons. The guidelines include the information necessary to establish an open and fair reporting culture that encourages people to speak up early when they have a concern. The steps covered in the guidelines are:

- *Define* who can report and what can be reported
- *Establish* a positive reporting culture
- *Identify* internal reporting channels and corresponding interfaces
- *Establish* effective mechanisms to ensure confidentiality and ways in which disclosures can be made anonymously
- *Institute* mechanisms to assess disclosures, investigate them internally and take the necessary corrective actions
- *Protect* whistle-blowers effectively by
  - *preventing* retaliation, or
  - *stopping* retaliation if it has already occurred
- *Establish* mechanisms to address retaliation
- *Provide* guidance, support and feedback to whistle-blowers
- *Provide* training on and raise awareness of the newly established reporting processes
- *Consider* sustainable and innovative ways in which whistle-blower protection policies may evolve within the organization

It is important to emphasize that there is no one-size-fits-all solution. Policymakers should take into consideration a variety of factors, which cater to both the specific context in which the whistle-blower protection policy is drafted by the organization and the unique cultural and societal norms that apply in each country.

Such policies can be elaborated and enforced by an organization even when the country where the organization is located has not adopted legislation on whistle-blower protection. Where such laws exist, the policy should include clear references to them in order to properly inform potential whistle-blowers.

[8] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons* (Vienna, 2015).

INTRODUCTION

On 11 March 2020, the World Health Organization (WHO) declared the outbreak of the coronavirus disease (COVID-19), a respiratory illness caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), a pandemic.[1] The resulting global health crisis forced States to take emergency measures to contain and mitigate the spread of the virus. As the risk of corruption in the health-care sector increases under such circumstances, the United Nations Office on Drugs and Crime (UNODC) warned that by taking such emergency measures, Member States had necessarily relaxed safeguards by trading compliance, oversight and accountability for speed of response and achievement of rapid impact, thus leading to the creation of significant opportunities for corruption to thrive.[2]

The health-care sector is already considered vulnerable to corruption under normal circumstances.[3] However, this vulnerability is amplified in times of health crises. Corruption can even exacerbate an outbreak or the spread of a virus and undermine efforts to contain a pandemic.[4]

The focus of the present guidelines is on the importance of establishing an internal policy for whistle-blower protection in the health-care sector in order to detect serious instances of wrongdoing, including corruption, that may occur, is occurring or will occur within an organization, address them as early as possible and take measures to mitigate their negative impact, including on patient safety and the organization's reputation and finances.

The guidelines are intended for all organizations in the health-care sector, whether public or private,[5] that wish to adopt an effective whistle-blower protection policy. While the guidelines can serve as a guide on how to draft such a policy, they are not intended to be a policy template. The specific target audience of these guidelines is an organization's management, policymakers, compliance officers and any other persons who are in charge of deciding, drafting and adopting internal policies and ensuring their effective implementation.

Readers are guided through the process of adopting a whistle-blower protection policy, including determining who can disclose information, what can be disclosed and how, implementing effective protective measures, providing guidance and feedback to the whistle-blower, completing an internal investigation and taking corrective action. The guidelines also inform readers as to how to provide the necessary training and raise awareness among all personnel of an organization and establish a positive reporting culture.

As demonstrated in the guidelines, an organization can establish a reporting mechanism and corresponding protective measures even in the absence of a legislative framework in the countries where it is located. While the focus of these guidelines is on the health-care sector, they may benefit organizations in other sectors as well.

---

[1] UNODC, "Accountability and the prevention of corruption in the allocation and distribution of emergency economic rescue packages".

[2] Ibid.

[3] Mackey, Vian and Kohler, "The sustainable development goals as a framework to combat health-sector corruption".

[4] See, for instance, the role that corruption is alleged to have played during the Ebola crisis, Anti-Corruption Resource Centre, "Ebola and corruption overcoming critical governance challenges in a crisis situation", *U4 Brief*, No. 4 (March 2015).

[5] Companies should also promote the detection and reporting of violations of their anti-corruption programmes. For more information, see UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide* (Vienna, 2013), p. 82.

PART ONE.

ESTABLISHING A WHISTLE-BLOWER PROTECTION POLICY

Chapter 1.

WHO IS A WHISTLE-BLOWER?

Prior to designing any policy, implementers should ensure that any policy they develop is compliant with domestic legislation. Implementers should conduct a review of domestic law in the following areas:

- Dedicated whistle-blower and/or protected disclosures legislation
- Anti-corruption legislation, including financial-services-related legislation
- Public service administration legislation
- Any other legislation related to access to information and data protection which may apply to the organization

Subject to such a review, every organization that wishes to adopt a policy to establish reporting channels for legal and administrative wrongdoing, as well as provide protection to persons who disclose reportable wrongdoing, needs first to determine who can report.

Excessively limiting the definition of a whistle-blower could render protective measures ineffective.

In article 33 of the United Nations Convention against Corruption, the term "whistle-blower" is intentionally not used; the broader term "reporting persons" is used instead. The Council of Europe defines "whistle-blower" as "any person who reports or discloses information on a threat or harm to the public interest in the context of their work-based relationship, whether it be in the public or private sector".[6] 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 (also known as the European Union whistle-blower directive) provides that the term "whistle-blower" applies to "reporting persons working in the private or public sector who acquired information on breaches in a work-related context".[7] Many jurisdictions do not use the term "whistle-blower". For instance, under the Public Interest Disclosure Act of 1998 of the United Kingdom of Great Britain and Northern Ireland, the term is not used; instead, reference is made to employees or workers

[6] Council of Europe, recommendation CM/Rec (2014)7 of the Committee of Ministers to member States on the protection of whistle-blowers, adopted by the Committee on 30 April 2014.

[7] European Union, 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, *Official Journal of the European Union*, L. 305 (26 November 2019), art. 4. This directive applies to a wide range of key European Union policy areas where breaches of European Union rules may cause harm to the public interest, including the area of public health.

who disclose information in the public interest.[8] According to one of the most frequently cited academic definitions, "whistle-blowers" are "organization members (former or current) [who disclose] illegal, immoral or illegitimate practices under the control of their employers to persons or organizations that … effect action."[9]

1.1 A MEMBER OF THE ORGANIZATION

In practice, a whistle-blower is often a member of an organization who becomes aware of acts of wrongdoing in work-related contexts and decides to report them.

The following categories of health-care professionals working in the private[10] or public sector should therefore be included, at a minimum, in the definition of a reporting person:

- Personnel of the Ministry of Health, including civil servants, permanent and temporary staff, administrative staff, assistants, secretaries, facility management personnel, interns and volunteers
- Personnel of health regulators and/or health-care authorities
- Personnel of public and private pharmaceutical companies
- Personnel of public and private health insurance companies
- Personnel of public and private laboratories
- Health- and social-care workers and practitioners
- Personnel of hospitals and other health service facilities
- Members of local and national governing health boards
- Emergency and transport services personnel (ambulance drivers, paramedics, etc.)
- Personnel of providers and distributors of drugs and medical supplies
- Personnel of companies and organizations involved in the production, trade, sale and distribution of health-related products
- Personnel from civil society organizations related to the health-care sector (Médecins sans frontières, the International Federation of Red Cross and Red Crescent Societies, etc.)[11]

While the policy should focus on "organization members", it should include all categories of personnel, without limitation. As such, the following categories of personnel should be able to report potential wrongdoing: permanent and temporary employees, consultants, contractors, experts, interns, facility management workers and volunteers.

In other words, all individuals internal to the organization should be entitled to report instances of legal and disciplinary wrongdoing of which they may be aware.

[8] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*.

[9] This definition was developed by Maria P. Miceli and Janet P. Near in 1985 and is still, to date, the most widely used academic definition. See Maria P. Miceli and Janet P. Near, "Organizational dissidence: The case of whistle-blowing", *Journal of Business Ethics*, vol. 4, No. 1 (February 1985).

[10] UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business*, p. 82.

[11] The terms in this list should be read in conjunction with the definitions provided in the glossary of terms on pages vii and viii of the present guidelines.

For example, the National Health Service (NHS) of the United Kingdom defines a whistle-blower as "an individual who works for an NHS organization". The definition also includes "agency workers, temporary workers, students and volunteers".[a]

The United Nations policy on protection against retaliation for reporting misconduct and for cooperating with duly authorized audits or investigations applies to "any staff member (regardless the type of appointment or its duration), intern, United Nations volunteer, individual contractor or consultant".[b]

[a] United Kingdom of Great Britain and Northern Ireland, National Health Service (NHS) England, "External Whistle-blowing Policy", (February 2017).

[b] Secretary-General's bulletin on protection against retaliation for reporting misconduct and for cooperating with duly authorized audits or investigations, ST/SGB/2017/2/Rev.1, sect. 2.1.

In addition, the policy should include current and former members of the organization, as well as job applicants who may observe wrongdoing or malpractice during the recruitment process or other pre-contractual negotiations.[12]

In defining the term "whistle-blower", it is important that organizations provide clarity so that prospective reporting persons may easily determine the scope and remit of the policy.

1.2 INDIVIDUALS EXTERNAL TO THE ORGANIZATION

The policy may also expand the scope of reporting persons to include external individuals who are not employed by the organization but may be aware of instances of wrongdoing in a business or contractual context. This category can include, for example, intermediaries, business partners, service providers and suppliers, candidates in a public procurement process, patients of a hospital or their relatives and clients of a pharmaceutical company. It is important that the persons drafting the organization's whistle-blower protection policy take into account how the policy will be disseminated to external individuals, how reports from external individuals may be received and handled and what, if any, means of redress may be available.

During the coronavirus disease (COVID-19) crisis, new actors have come to light and are playing a key role in the purchase and distribution of essential medical supplies (e.g., face masks and gloves). Owing to the urgency of the situation, Governments and private companies have appointed intermediaries to contact foreign companies and make purchases on the international market on their behalf. Limiting the scope of individuals that can report may leave these vulnerable operations out of the remit of the reporting mechanism. A robust policy should be developed in such a way that it can be applied under exceptional circumstances.

Irrespective of the existence of a law on whistle-blower protection, each organization or entity listed above will need to have a stand-alone policy for its own personnel. Moreover, a broader sectoral policy applicable to multiple organizations working at the same echelon of the medical supply chain could be envisaged. However, organizations that decide to implement such policies may face challenges, as they may have to harmonize or unify their procedures in order to ensure consistent reporting and handling of reports.

[12] See, for example, European Union, Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 4, para. 3.

Chapter 2.

WHAT CAN BE REPORTED?

A policy on whistle-blower protection must detail the types of wrongdoing that can be reported. Even if an organization is based in a country that has adopted legislation on whistle-blower protection, such legislation may not be specific enough. For instance, some laws refer to the possibility of reporting a matter of "public health and safety", but most refer to matters of "public interest" or "general interest".[13]

Some whistle-blower protection laws cover the following types of potential wrongdoing:

- Creating and presenting a danger to public health, safety or welfare
- Committing an act of gross mismanagement, gross waste of public funds or gross neglect of duty

Therefore, it can be difficult to directly implement a law or regulation at an institutional level. The role of a policy is also to provide further information and details on the types of wrongdoing that can be reported internally, in line with the concerns and specificities of the organization.

The term "wrongdoing" is defined in the present guidelines as reportable misconduct that includes actions but may also include omissions (not doing something).

For instance, in the public interest disclosure (whistle-blower) policy of the Australian Health Practitioner Regulation Agency (AHPRA), a "public interest disclosure" is defined as a disclosure of information about a person, public officer or public body which shows, or tends to show, improper conduct or corruption. The policy provides examples of improper conduct that may give rise to a public interest disclosure, including conduct that:

- Is illegal
- Is a substantial misuse or waste of AHPRA or Board money or resources
- Is serious misconduct in performing a function under national law

[13] See, for instance, France, Law No. 2016-1691 of 9 December 2016 relating to transparency, anti-corruption measures and the modernization of economic life, art. 6.

- Is maladministration that adversely affects a person's interest in a substantial or specific way
- Is a substantial and specific danger to the health or safety of the public
- Presents a substantial and specific danger to the environment[a]

[a] Australia, Australian Health Practitioner Regulation Agency (AHPRA), "Public Interest Disclosure (Whistleblower) Policy" (May 2020).

2.1 DETERMINING THE TYPES OF WRONGDOING THAT CAN BE REPORTED

Defining the scope of wrongdoing to be included in the policy

Detecting and countering corruption within an organization is one of the main goals of a whistle-blower protection policy. However, the policy should not limit reportable wrongdoing to corrupt activities.

First, an act of wrongdoing can be very serious without being an act of corruption.

For instance, the failure of a health-care centre employee to sterilize surgical instruments is probably not an act of corruption, but it constitutes a danger to the health and safety of other health-care personnel and patients.

Second, an instance of wrongdoing may look like an administrative or procedural violation at first, but may turn out to be part of a larger corruption scheme after investigation.

For instance, between 1976 and 2009, France marketed a "weight-loss" drug called Mediator. Although it was originally designed for overweight people with diabetes, the anorexic (appetite suppressant) and hypolipidemic agent was a particularly attractive prescription medication option for individuals who just wanted to lose some weight. In 2007, Dr. Irène Frachon, a pulmonologist at a public hospital in Brest, observed an increasing number of cases of heart disease among her patients and realized that all the affected patients had been treated with Mediator. After a long epidemiological study which confirmed her concerns, she reported the matter to her superiors and to the National Agency for the Safety of Medicines and Health Products. Following this report and the withdrawal of the drug from the market in 2009, further investigations conducted by law enforcement authorities revealed suspicions of fraud on the part of Servier Laboratories, which was marketing the drug. The trial started in 2019.

In addition, the so-called infected blood scandal in France began in April 1991, when doctor and journalist Anne-Marie Casteret published an article in the weekly magazine *L'Événement du jeudi* proving that the National Blood Transfusion Centre had knowingly distributed blood products contaminated with HIV to haemophiliacs in 1984 and 1985. The judicial proceedings revealed large-scale acts of corruption and fraud-related offences, including acts committed outside France. For instance, some Governments had delayed the commercial availability of a blood test used in the United States of America in favour of one being developed in France. In 1999, then Prime Minister Laurent Fabius of the Socialist Party, then Minister of Social Affairs Georgina Dufoix and then Minister of Health Edmond Hervé were charged with manslaughter.

In addition, limiting reportable wrongdoing to corruption may force individuals who detect such wrongdoing to ascertain whether it constitutes an act of corruption before reporting. Such a situation can expose those individuals, their colleagues and even their relatives to risk.

Therefore, it is essential for the organization to determine which categories of wrongdoing, beyond fraud, corruption and abuse, can be reported by its members.

When defining the categories of wrongdoing to be included in the whistle-blower protection policy, the organization should consider the following three points:

1. Personal grievances are not typically included in the scope of reportable wrongdoing under whistle-blower protection laws and policies. Nevertheless, reporting on those issues should also be enabled. A separate reporting policy should be developed in this regard.

> For instance, the public interest disclosure (whistle-blower) policy of AHPRA provides that, if individuals have a personal grievance regarding AHPRA or a Board that does not involve serious misconduct, they are strongly encouraged to pursue the remedies designed to deal with such grievances. For example, if their concern relates to a particular decision under national law, they are invited to file complaints or offer feedback using the procedures set out on the Complaints and Feedback page of the Agency's website.[a]
>
> [a] Australia, Australian Health Practitioner Regulation Agency (AHPRA), "Public Interest Disclosure (Whistleblower) Policy" (May 2020).

   However, the reporting of personnel matters such as conflicts between the reporting person and another member of personnel,[14] performance-related grievances and other human-resources-related issues could constitute whistle-blowing if such matters are assessed to be hazardous to the health and well-being of personnel and users of health-care services. Cases of bullying and harassment should also be included because of their impact on the well-being of staff and patients. Bullying and harassment can also be used as a form of retaliation when individuals raise concerns. In all cases, these acts are sufficiently serious to fall within the scope of reportable wrongdoing.

2. The policy should allow the reporting of instances of wrongdoing that have happened, are happening or are likely to happen, as well as attempts to conceal such acts.[15]

3. The policy should specify that any clauses of confidentiality or non-disclosure that individuals may have in their contract with the organization will not apply to reportable categories of wrongdoing included in the policy.

Indicating a threshold of seriousness

The cost of protecting a whistle-blower can be high. Significant amounts of financial and human resources must be allocated to ensure effective prevention and suppression of retaliation. This has led many jurisdictions to establish a threshold of seriousness that the reported information must meet. While some countries have chosen to include the concept of public interest in their laws, others have included terms such as "gross" or "serious" when defining reportable categories of wrongdoing.

Irrespective of the approach used, only individuals who report certain types of behaviours should be protected. Therefore, it is important to indicate a threshold of seriousness when classifying behaviours that constitute reportable wrongdoing.

> For instance, a member of personnel who reports that a colleague took home a pen from the office's set of supplies does not merit whistle-blower protection.

[14] See, for example, European Union, Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, recital 22.

[15] Ibid., art. 5, para. 2.

Nevertheless, laws and policies should not impose excessive limitations on the information that can be reported, or they could be rendered ineffective.

With regard to corruption-related offences, some countries do not criminalize cases of de minimis corruption. However, it is strongly encouraged that such cases still be included in the scope of reportable wrongdoing in the context of whistle-blower protection. In addition, widespread and systematic corruption, whatever its scale, can have a detrimental impact on the delivery of health-care services[16] and should be considered as meeting the threshold of seriousness required to constitute reportable wrongdoing.

The organization must define what it considers to be "gross" or "serious" wrongdoing

The more rigorous the requirements to assess the quality and seriousness of information prior to reporting are, the more likely it is that people will remain silent – particularly if they are uncertain as to whether they will be protected[17] – or take unnecessary risks by assessing or investigating the information by themselves. Uncertainty about the seriousness of the allegations might discourage reporting. Reporting persons should not be required to provide positive evidence; instead, it should be sufficient for them to raise reasonable concerns or suspicions. In addition, personnel should be encouraged to raise their concerns at an early stage rather than waiting for proof.

It is therefore important to clearly determine what is considered "gross" or "serious" wrongdoing in an organization. For this purpose, some organizations have included in their policies a non-exhaustive list of reportable types of wrongdoing that meet these criteria.

In the health-care sector in particular, established laws and regulations often define "gross" or "serious" wrongdoing as behaviours that present a risk for public health and safety.[18] In the United States, reportable violations are defined as "practices that threaten public health and safety".[19]

> For instance, to use the previous example, in a hospital context the term "office supplies" can also include the stock of medicines or substances used to treat patients. These substances can be extremely dangerous and must be used with caution. If a staff member, such as a health-care worker, sees a colleague taking such substances without apparent justification, such behaviour could be reported, as it constitutes a potential threat to health and safety.

It is important to keep in mind that references to "health" and "safety", among other terms, are more easily understandable for lay persons, and organizations should strive to use such uncomplicated and simple language when defining "gross" or "serious" wrongdoing.

[16] Sarah Brierly and Elif Ozdemir, "Petty corruption in the provision of public services in Ghana", Washington University in St. Louis, for Strengthening Action against Corruption (STAAC)–Ghana. Available upon request from STAAC–Ghana (Foreign, Commonwealth and Development Office (formerly Department for International Development)).

[17] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*.

[18] See, for example, recommendation CM/Rec (2014)7 of the Committee of Ministers of the Council of Europe to member States on the protection of whistle-blowers, adopted by the Committee in April 2014. More detailed information can be found in UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons.*

[19] United States of America, National Nurses United, "Whistleblower Protection Laws for Health-care Workers".

2.2 DETERMINING WHAT EXACTLY CONSTITUTES SERIOUS WRONGDOING IN THE ORGANIZATION

Once the organization has decided that reportable wrongdoing must, first, not be limited to corrupt activities and, second, meet a threshold of seriousness, it is important to determine the types of wrongdoing that will be included in the policy.

Therefore, before adopting a whistle-blower protection policy, the organization may be required to conduct an internal risk assessment to determine the types of wrongdoing that can occur within it that may either lead to corruption or present a serious risk for public health and safety.

Depending on the organization and its specific position in the health-care supply chain, these violations may include:

- Violations of health and safety regulations
- Disregard for procurement procedures for health-care and medical supplies
- Direct bribes from patients to health-care personnel
- Tampering with and manipulation of invoices and bills so that they show incredibly low or incredibly high amounts
- Purchase of supplies that do not seem to correspond to those planned for acquisition or to their intended use
- Receipt or distribution of expired, fake or adulterated drugs
- Unnecessary medical treatments
- Undue preferential treatment of private medical suppliers
- Unsafe patient care
- Poor clinical practice or other malpractice which may harm patients
- Failure to safeguard patients
- Misadministration of medication
- Untrained personnel
- Unsafe working conditions
- A culture of harassment, discrimination, abuse and exploitation (including based on gender and race)

For instance, a staff member of the Ministry of Health participating in the procurement process for medical supplies realizes that the committee appointed to select the winning bidder does not have any medical expertise that could verify the appropriateness of the supplies offered by the candidates. Such a situation should be considered reportable, as it creates a risk that the medical supplies purchased may not correspond to the prescribed standards, or that they may be expired or falsified.

Under the policy of the World Health Organization (WHO) on whistle-blowing and protection against retaliation, reportable wrongdoing is defined as "wrongdoing that implies a significant risk to WHO (i.e., [that is] harmful to its interests, reputation, operations or governance)". Accordingly, the policy applies to, but is not limited to, the reporting of any of the following:

- Fraud (i.e., deliberate and deceptive acts with the intention of obtaining an unauthorized benefit, such as money, property or services, through deception or other unethical means)
- Corruption
- Waste of resources
- Sabotage

- Substantial and specific danger to public health or safety
- Sexual exploitation and abuse[20]

It is worth mentioning that some organizations also include the possibility of reporting concerns about specific health and safety measures taken or enforced during the COVID-19 pandemic.[21]

2.3 DEFINING AND IMPLEMENTING THE ELEMENT OF GOOD FAITH

The concept of good faith is sometimes included in national legislation or in organizations' policies in order to ensure that individuals do not knowingly report information that is untrue and might be aimed at harming or discrediting a person through intentionally false allegations, by making provisions to prevent and/or punish such reporting. Such behaviour, while likely to be rare, must not be accepted, and the policy established by the organization should also provide for processes, including disciplinary processes, to prevent persons from reporting such information.

The requirement of good faith in the context of whistle-blower protection should be considered to be met when a person has reasonable grounds to believe that the information disclosed is true.[22] In this regard, ensuring that the concept of good faith is linked to the information and not to the motive of the report is considered a good practice.

The United Nations Convention against Corruption provides, in its article 33, that reports must be made "in good faith and on reasonable grounds".

The Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistle-blowers and Witnesses of the Organization of American States (OAS) goes further and provides for the presumption of good faith for whistle-blowers. This legislative practice shifts the burden of proof onto the accused by requiring him or her to demonstrate that no violation occurred, and protects the whistle-blower.

In most recent texts, such as the European Union directive on the protection of persons who report breaches of Union law, the concept of good faith has been replaced with references to "reasonable grounds". The concept of reasonable grounds can reduce the risk of misinterpretation and undue focus on the motive of the reporting person. In response to the directive, countries throughout the European Union are adopting the concept of reasonable grounds, replacing the term "good faith" with references to that concept wherever the term appears in current law.

What if the information is ultimately found to be untrue?

If the information reported is found not to constitute a violation after the conclusion of the investigation (or fact-finding process), no action should be taken against the whistle-blower or the reporting person.

Good faith or reasonable grounds are evaluated at the time of disclosure; what matters is that whistle-blowers believe that the information is true at the time that they report it.

> To once again use the example of the health-care worker who takes medical supplies from the hospital stock without apparent justification, this action may ultimately be determined to be perfectly justified. No action should be taken against the person who reported the information, since it was reported with the belief that it was true, or against the person who was the subject of the reported information.

[20] World Health Organization (WHO), "Whistle-blowing and protection against retaliation: policy and procedures" (2015). See also Nieves Zúñiga, "Gender sensitivity in corruption reporting and whistleblowing", *U4 Helpdesk Answer*, No. 10 (June 2020).

[21] One such organization is the Occupational Safety and Health Administration (OSHA) of the United States Department of Labor. See OSHA, "Whistleblower laws enforced by OSHA", available at www.whistleblowers.gov/.

[22] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*. See also "Frequently asked questions: 'Does the intention behind the disclosure matter?'", available at https://whistleblowerprotection.eu/.

What if the reporting is done in bad faith?

When included in national legislation or in the policy of an organization, the concept of good faith should be linked to the information, not the whistle-blower. As stated previously, the motive for reporting should be irrelevant[23] if the reporting person meets the above-mentioned criteria and believes that the information is true at the time of reporting.

Therefore, it does not matter whether the personal relationship between the reporting person and reported person is good or bad; what matters is that the person disclosing the information believes it to be true.

For instance, a person can report a violation committed by a supervisor even if it is known that the two individuals dislike each other. The person might even seek the dismissal of the supervisor in the hope of gaining a promotion. However, this motivation should not be taken into consideration if the reporting person really believes that the information is true.

[23] Ibid.

Chapter 3.

WHERE TO REPORT AND HOW?

Most national anti-corruption legislation provides for the possibility of reporting acts of corruption to law enforcement authorities (such as the police, the Public Prosecutor's Office or anti-corruption authorities) or to an ombudsperson, as appropriate.

However, if an organization wishes to establish a whistle-blower protection policy, it is also important to create specific internal reporting channels to handle these reports. In fact, in some domestic legislation,[24] reference is made to the possibility of reporting to an employer (whether a supervisor, a special commission or authority, an external company responsible for receiving reports or any other person within the organization).

A strong internal policy that ensures such a possibility and allows personnel to safely report possible wrong-doing within their organization while protecting them from retaliation and reprisal is still necessary. Accordingly, organizations are invited to establish open and inclusive internal reporting channels that are accessible through various user-friendly reporting interfaces and ensure a high level of confidentiality.

3.1 ESTABLISHING INTERNAL, OPEN AND INCLUSIVE REPORTING CHANNELS

Depending on the status and situation of the organization, several channels could be established.

In some cases, if the organization is unable to establish an internal reporting channel, a reporting channel could be established within an independent oversight body.

For instance, in the area of public procurement, a reporting channel can be established within the Procurement Regulatory Authority.[a]

[a] Such is the case, for instance, in Greece, where a whistle-blowing platform has been established within the Hellenic Single Public Procurement Authority. For more information, see Hellenic Single Public Procurement Authority, "Whistle-blowing platform in public procurement", available at www.eaadhsy.gr.

[24] See, for instance, Ghana, Whistleblower Act (Act No. 270) (2006), sect. 3.

However, to the extent possible and depending on its status (whether it is public or private), it is always recommended that the organization establish internal reporting channels for the reasons set out below.

First, the establishment of such channels is considered an international good practice as it is "part of good and transparent management, accountability and governance",[25] in particular in the public sector. In some jurisdictions, it is mandatory for certain corporations in the private sector to have internal reporting channels in order to be publicly listed on stock markets.[26]

Second, internal reporting channels allow organizations to be informed of wrongdoing at an early stage, enabling them to take timely mitigation measures in the hope of avoiding the need for an investigation.

Third, when instances of wrongdoing are reported in branches of large multinational companies located in different countries, internal reporting channels offer a faster, more tailored and more efficient response than national authorities, whose jurisdiction may be limited to instances of wrongdoing that take place in a specific location.

Although every policy established by an organization should include internal reporting mechanisms, the staff members of an organization do not always feel comfortable reporting certain acts of wrongdoing directly to their supervisor, or doing so in person.[27] In order to address this issue, the term "internal reporting" should be broadly defined and should not only refer to the disclosure of information, in person, to direct supervisors.

In view of the above, recommended measures are outlined below.

First, the policy should allow direct reporting to the organization's management. In some cases, the policy should also allow for the possibility of reporting wrongdoing to senior managers above the direct supervisor. This option should always be among the possible reporting channels established by the policy.

Second, the organization could also explore the viability of establishing an internal, independent unit dedicated to receiving allegations of wrongdoing. For instance, it could create a dedicated unit within the compliance department for that purpose.

Third, the organization should identify the independent bodies, if any, that are in charge of receiving reports in their sector, and designate them as possible reporting channels. Such bodies could include regulatory authorities (e.g., health regulators), offices of inspectors general, offices of auditors-general or other commissions. In the private sector specifically, the role of the Chamber of Commerce could be considered. In some countries, labour inspectors' offices are in a position to receive reports on some work-related administrative and legal violations.[28] Alternatively, since employees may not always feel comfortable exercising these options, companies can designate a highly trusted individual as an ombudsperson.[29]

Lastly, whistle-blower protection policies could also provide for "other internal reporting channels", such as external service providers that operate call centres or reporting hotlines. Organizations may wish to outsource these services to independent external companies. This option is often found in the private sector, as it offers a degree of independence and neutrality that other purely internal reporting channels might not have.

[25] Council of Europe, recommendation CM/Rec (2014)7 and explanatory memorandum on the protection of whistle-blowers (2014).

[26] In the United States, the Securities and Exchange Commission, taking into account section 406 of the Sarbanes Oxley Act (2002), adopted amendments to the Code of Federal Regulations (CFR), notably 17 CFR parts 228 and 229, which require companies to adopt codes of ethics that also provide for internal reporting. For example, as a result of those amendments, the National Association of Securities Dealers Automated Quotations (NASDAQ) (equity rule 5610) and the New York Stock Exchange (NYSE) (listed company manual section 303.A10) require listed companies to develop procedures to enable employees to report illegal wrongdoing.

[27] See, for instance, in relation to the private sector, UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business*, p. 82.

[28] Such, for instance, is the case in France, pursuant to art. L8113-5 of the Labour Code.

[29] UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business*.

In summary, the organization has several options in terms of the reporting channels it can designate:

- The option of directly reporting instances of wrongdoing to management (i.e., superiors), which should not be limited to people directly above the whistle-blower
- Establishing an independent unit within the organization dedicated to receiving allegations of wrongdoing, for example, within the compliance department, where applicable
- Designating a highly trusted ombudsperson or other independent body, including regulatory authorities, where relevant, to receive reports
- Engaging the services of an external independent service provider

It is considered a good practice for organizations to include several reporting channels in their policy for persons wishing to report wrongdoing. The option of reporting to management must always appear as one of the possible options. Consequently, the training of managers is an essential component of any whistle-blower protection policy. Therefore, at the very least, personnel with managerial responsibilities should be provided with information and training on how to receive such reports and what to do with the information received.[30] Personnel are more likely to trust a system in which the receiver of the information has received appropriate training.

It is noteworthy that a lack of protection, a fear of reprisals and the level of confidentiality can, in some instances, have a greater impact on women when they are deciding whether or not to report wrongdoing.[31]

Therefore, regardless of the size of the organization or the nature of its activities, it is critical for reporting channels to be inclusive of all members and gender-responsive in nature.[32] Accordingly, organizations should consider ways to create effective channels through which wrongdoing can be reported, while addressing the varied needs and vulnerabilities of men, women and minority groups. Organizations should also use inclusive language and communication and develop gender-sensitive and visible channels of communication to report wrongdoing.[33] The availability of a range of reporting channels will help to address gender differences in reporting preferences, and the recipients of reports should be trained to provide tailored attention.[34]

Finally, organizations should bear in mind that the recipient of the information may also be authorized to receive, request and investigate information concerning potential wrongdoing. This authority varies according to who is in charge of receiving the information and that person's responsibilities. Superiors and compliance departments, for instance, can take immediate protective measures, while external service providers may only be able to advise the organization to take such measures. Therefore, the training provided should cover not only how to receive reports of alleged wrongdoing, but also what to do with such reports (written and/or verbal). In addition, superiors should be trained on how to communicate the information and to whom (i.e., which entity/authority is designated by the policy as responsible for handling reports and initiating investigations), while ensuring, where appropriate, that the confidentiality of the name and identity of the whistle-blower is guaranteed and maintained. Policies should grant the status of whistle-blower to those who report through the appropriate channels and should ensure the anonymity of such persons.

[30] See part three of the present guidelines.

[31] Brierly and Ozdemir, "Petty corruption in the provision of public services in Ghana".

[32] Sir Robert Francis QC, *Freedom to Speak Up: An independent review into creating an open and honest reporting culture in the NHS*, February 2015, p. 21.

[33] Zúñiga, "Gender sensitivity in corruption reporting and whistleblowing".

[34] Ibid.

3.2 CREATING ACCESSIBLE AND USER-FRIENDLY REPORTING INTERFACES

When the organization has determined the best type of reporting channels, taking into account its status and structure, it should then establish different reporting interfaces. Individual members of personnel within an organization may feel more comfortable with certain interfaces, such as face-to-face meetings, telephone calls, recorded messages, emails, online platforms or even smartphone applications.[35]

A good reporting mechanism provides for a wide range of interfaces, allowing individuals to choose the interface they feel most comfortable using. If face-to-face meetings are available, organizations should consider where these will be held, taking into account the transportation-related and/or financial challenges people may face if they are located outside of big cities.[36] If a telephone interface is provided, it is important that the service be available 24/7. These measures are particularly essential for ensuring an inclusive, gender-sensitive and gender-responsive environment in which all persons wishing to report instances of wrongdoing can feel comfortable doing so in a manner that is appropriate for them, regardless of their sex, gender, rank, grade or other social or cultural factors or status.

The interfaces must be adapted to the specificities, culture and work environment of the organization, as well as to the external social context. For example, health-care personnel in hospitals work in complex environments with significant time pressure; they also do not have much time alone. If a hospital wishes to establish efficient reporting channels, it should provide health-care workers with reporting interfaces that can be used under such conditions. In this case, the option of reporting through a smartphone application or by text message should be considered.

If the reporting process is long, complicated or needs to be done by phone or in person, the members of an organization may not only feel uncomfortable and refrain from reporting, but may also simply not have sufficient time to do so.

During public health crises such as the COVID-19 pandemic, it is also important to consider limitations on the free movement of people. A policy that does not provide for remote reporting interfaces could render all reporting channels useless. Reporting policies, in particular in the health-care sector, should provide for the possibility of reporting through email, websites, mobile applications, text messages and, if no remote resources are available, even regular mail.

For instance, the Occupational Safety and Health Administration (OSHA) of the United States Department of Labor has created a dedicated web page to allow the reporting of health and safety concerns during the COVID-19 pandemic. The web page offers several means of filing a complaint: online, by mail, by fax, by email, by telephone or in person.[a]

[a] United States, OSHA, Department of Labor, "File a complaint", available at www.osha.gov/workers/file_complaint.html.

3.3 ENSURING CONFIDENTIALITY THROUGHOUT THE REPORTING PROCESS

Organizations have an array of options when it comes to establishing reporting channels. The options described above can take many forms depending on the status and structure of the organization, as well as its position in the health-care supply chain.

When deciding which reporting channel is best suited to its needs, the organization should consider:

1. Offering several options to personnel so they can choose the one they feel the most comfortable with.

[35] UNODC, *Reporting Mechanisms in Sport: A Practical Guide for Development and Implementation*, 2019.

[36] Zúñiga, "Gender sensitivity in corruption reporting and whistleblowing", 2020: www.u4.no/publications/gender-sensitivity-in-corruption-reporting-and-whistleblowing.pdf.

2. Ensuring that reporting channels are established and operated in a "secure manner that ensures confidentiality"[37] and that whistle-blowers can report wrongdoing "in confidence and without fear of reprisal".[38]

In addition to establishing several reporting channels and interfaces, a good whistle-blower protection policy should also be supported, promoted and driven by leadership and/or management, and should provide for the following reporting methods:

- *Open reporting,* where individuals openly report or disclose information, or state that they do not endeavour to ensure or require that their identity be kept secret.
- *Confidential reporting,* where the name and identity of the individual disclosing the information is known by the recipient but will not be disclosed without the individual's consent, unless required by law.
- *Anonymous reporting,* where a report or information is received, but no one knows the source.[39]

Ensuring a high level of confidentiality is essential for an effective whistle-blower protection policy.

Often, the whistle-blower will continue to work in the organization after reporting the alleged wrongdoing and will face difficult situations, owing to factors such as a sense of loyalty to colleagues and supervisors, contractual confidentiality obligations and the risk of retaliation. Therefore, it is paramount to ensure confidentiality, not only with respect to the identity of the whistle-blower, but also with regard to the disclosure itself.

Confidential reporting

As mentioned above, in the case of confidential reporting, the name and identity of the individual who disclosed information is known by the recipient, but will not be disclosed without the individual's consent, unless required by law.

If the organization chooses to entrust an external service provider with receiving the reports of alleged wrongdoing, it needs to ensure that such a provider can offer the necessary confidentiality safeguards.[40]

In the event of breaches of these confidentiality obligations, the policy should also provide for penalties. Furthermore, corrective action, including termination, must be provided for in order to prevent retaliation and/or the release of protected information. In some instances, organizations may wish to include civil liability clauses and grounds for termination in contracts signed with external service providers and, when required, may refer cases to the appropriate government agency.

It is important to remember that reports will be examined by independent investigators or units and, as such, any information that could compromise the confidentiality of the reports should be avoided. Consequently, the names of reporting persons should not appear in any document pertaining to the report, and their personal information should be kept separately in a secure location (whether physical or electronic). Special care should be taken in the drafting of reports, which should be written in such a way as to avoid explicitly or implicitly revealing the identity of the whistle-blower (e.g., by indicating the location of the whistle-blower's office or how many years that person has been working in the organization).

[37] Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 9.

[38] Asia-Pacific Economic Cooperation, "APEC Anti-Corruption Code of Conduct for Business", September 2007, art. 4 *(g)*, also included in Organization for Economic Cooperation and Development (OECD), UNODC and World Bank, *Anti-Corruption Ethics and Compliance Handbook for Business*, 2013.

[39] UNODC, E4J University Modules Series: Anti-corruption, Module 6: Detecting and Investigating Corruption, "Whistle-blowing systems and protection", available at www.unodc.org/e4j/en/anti-corruption/module-6/key-issues/whistle-blowing-systems-and-protections.html.

[40] UNODC, *Reporting Mechanisms in Sport*.

A successful whistle-blower protection policy thus ensures that the identity of the reporting person will remain confidential at every stage of the process following the report of alleged wrongdoing. Organizations must be aware that their security and cybersecurity policies directly affect the protection of whistle-blowers and their information. If confidentiality is ensured, other measures might not be necessary (although they must always be made known and available).

To ensure confidentiality, it is necessary to define what "identity" means in the context of whistle-blower protection

When an organization establishes a whistle-blower protection policy, it should clearly define the concept of "identity" as it relates to the confidentiality principle or the adoption of mechanisms that enable reporting persons to remain anonymous.

Stricto sensu, "identity" refers to the name of the reporting person, but the concept must also be expanded to include other information that can lead to the identification of that person, including details such as address, telephone number (or the office phone extension), email address (including personal email address), as well as, in some cases, the department, unit or organization in which the person works and or the job role/title. If the unit or department is relatively small, such information may easily lead to the identification of the whistle-blower.

Moreover, some organizations might keep track of the websites that personnel visit while using their work computers, including whether they access the reporting website. Therefore, the definition of "identity" should also cover the Internet Protocol (IP) addresses of computers in such cases.

The information provided should also be treated with due professional care, including during the investigation (or fact-finding) phase,[41] as sometimes the type of information revealed can identify the reporting person. Sometimes only one person has access to the reported information; in such cases, the way in which information is handled is of paramount importance. Hence, as certain types of information can still lead to the identification of whistle-blowers even if confidentiality is ensured, initial recipients of reports (IRR) and investigators should provide whistle-blowers with an assessment of whether and how their confidentiality will be protected.

Furthermore, a good policy should not ensure confidentiality upon request only. Initial recipients of reports should therefore be trained to assess the level of risk that individuals may be taking by reporting instances of wrongdoing of which they are aware. Accordingly, even in cases where individuals openly report or disclose information without requesting that their identities be kept confidential, the receivers of those reports should be in a position to decide whether or not those persons' identities should be disclosed, depending on the level of potential risk to the whistle-blower. Such decisions should be taken in consultation with the reporting person.

Anonymous reporting

Even if the necessary safeguards and confidence-building measures are in place, some personnel will still fear exposure and subsequent retaliation. In some cases, personnel may also believe that the reporting mechanism in place is not there to protect them, but to test their loyalty to the organization. Thus, even when every effort has been made to ensure confidentiality, it may be impossible to build trust with all personnel.

In jurisdictions in which they are legally required to do so, organizations must allow personnel to report concerns anonymously. In other jurisdictions, organizations should strongly consider allowing anonymous reporting, unless such reporting is prohibited by law.

[41] See part two, chap. 5, of the present guidelines.

This option might encourage those who do not trust the mechanisms in place to step forward and report wrongdoing. However, the organization should also be aware of the shortcomings of anonymous reporting and make personnel aware of these potential risks, as outlined below:

- The information provided by the reporting person is limited and might not be sufficient to initiate an investigation.
- In some instances, interaction with the reporting person is not possible.
- More resources may be necessary to determine whether wrongdoing has occurred.
- The organization might not be able to protect the reporting person, given that the person's identity has been concealed by reporting anonymously.

Nevertheless, there are some measures that organizations can take to avoid some of these problems. For example, technology such as encrypted messaging platforms, secure online whistle-blowing platforms, anonymous reporting hotlines or mobile applications with anonymous reporting functions could be used to enable reporting persons to remain anonymous, while providing a channel of communication.

The World Health Organization allows individuals to report through an online portal, including anonymously, in which case it is specified that no attempt will be made to trace the reporting person's details at any time. However, even if they choose to remain anonymous, reporting persons can log back into the portal with the case number provided and the chosen password in order to receive feedback following the disclosure, and to provide further information based on any questions posted in the portal by the receivers of the report.[a]

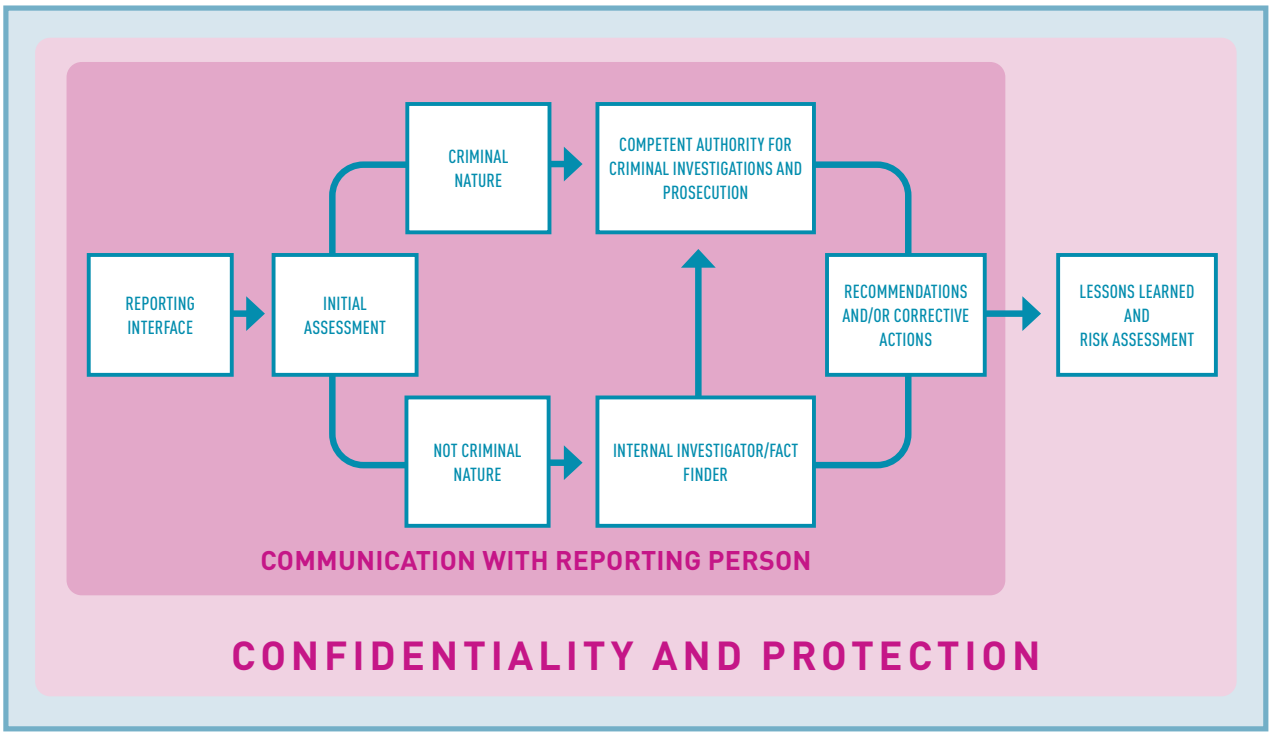
[a] For more information, see the online portal Expolink established by WHO, available at https://wrs.expolink.co.uk/integrity.

Organizations can also improve the quality of information received through anonymous disclosures by making staff aware of the details necessary to conduct an investigation. For example, this information could be communicated to prospective reporters in a checklist or decision-tree format, and could be highlighted in staff training sessions and disseminated via the intranet and other publication methods. Organizations can also design questions on reporting websites or mobile applications in such a way as to help obtain sufficient details. It is also important that call handlers at anonymous hotlines receive adequate training to ensure that they ask appropriate questions and obtain information in a systematic way.

PART TWO.

PROCESSING THE INFORMATION RECEIVED AND PROVIDING PROTECTION

The image below shows the different stages of a reporting process:



Chapter 4.

HANDLING A REPORT: INITIAL ASSESSMENT

Whistle-blower disclosures by personnel and others who fall within the definition of "whistle-blower" as set out in part one, chapter 1, can save lives as well as reducing or preventing financial and reputational losses to the organization.

Whistle-blowers play a critical role in keeping public and private entities honest, efficient and accountable. Given that whistle-blowers are a key source for the detection of waste, fraud and abuse and the protection of public health and safety, it is important to have a safe and inclusive process in place to encourage disclosures of wrongdoing.

To build trust within the organization, it is critical that the environment be designed to prevent others from discovering who the whistle-blower is and retaliating against the person, including through ensuring that reports are handled in a timely manner.[42]

It is important to ensure that the information provided by reporting persons is handled with swift and structured follow-up and that any further course of action undertaken is communicated to the reporting person.

4.1 ACKNOWLEDGING RECEIPT

Once a report of alleged wrongdoing is received through one of the interfaces established by the organization, the first step is to acknowledge receipt to the whistle-blower in writing. In the European Union whistle-blower directive, for instance, it is suggested that such acknowledgement of receipt should be sent within seven days.[43] Automatic responses, when considered, should be carefully designed. In some cases, the message may also include some preliminary information about the next steps and can also provide a holistic view of the process to the whistle-blower. While automatic responses can be an efficient way to speed up the process, a standardized message can be perceived by the whistle-blower as not being a real reply. Whistle-blowers frequently need to feel sure that someone is taking care of the case and that the information was received correctly.

[42] For research on the effects of timely responses in health care, see Paul Rauwolf and Aled Jones, "Exploring the utility of internal whistleblowing in healthcare via agent-based models", *BMJ Open*, vol. 9, No. 1 (January 2019).

[43] Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 9, para. 1 *(b)*.

While acknowledgements can take various forms, the following is an example of a reply that could be sent when a report is made:

> I am writing to let you know that I have received your report regarding [insert wording from the report].
>
> Thank you for reporting your concerns. I will attempt to respond to you within 10 days.
>
> I may need to speak to you in the future. In the meantime, if you have anything further to add or if you have any further questions, please do not hesitate to contact me.[a]
>
> [a]UNODC, *Reporting Mechanisms in Sport*.

4.2 ASSESSING THE REPORT

Once a concern has been received, it should be recorded in a systematic way. Initial recipients of reports (IRR) and investigators must be familiar with, and use, consistent terminology across the organization, and it is preferable for all cases to be recorded in a secure case management system. The concern must be assessed to determine: whether it falls under the definition(s) of reportable wrongdoing; which entity is best suited to handle or investigate the allegations and conduct the investigation (if several entities exist), depending on the type of wrongdoing (mostly in the public sector); and the level of urgency. Once the information has been deemed reportable under the whistle-blower protection policy,[44] four questions must be answered:

- Who will communicate with the reporting person?
- If whistle-blower protection is granted, what measures are needed to maintain confidentiality and ensure protection?
- Which entity will look into the potential instances of wrongdoing, if there is more than one with such power?
- How will the report be classified?

Therefore, it is important that the person who first receives the allegations is highly trained on how to react and on what questions can or need to be put to the whistle-blower.[45]

In the private sector specifically, IRR should also be trained on the organization's field of expertise, its core business and technical aspects and, to some extent, be familiar with technical terms and jargon, especially if the IRR are from an external service provider. In the case of multinational companies, IRR should also be made aware of different working practices and cultural norms in the countries where the organization operates. Indeed, while a whistle-blower may try to use generic terms, the explanation of the wrongdoing and the circumstances surrounding it may require the use of technical terminology or descriptions of specific situations that could be difficult for a person outside the organization to understand. This is especially the case for the health-care sector, where technical information can be highly specific. IRR must also build a relationship of trust with the reporting person. The reporting person must feel comfortable and confident, especially during face-to-face meetings or telephone calls. In this regard, IRR should be able to explain in detail how the information provided is going to be treated and what protections are in place for the whistle-blower.

[44] See part one, chap. 2, of the present guidelines.

[45] See part three of the present guidelines.

During the assessment of the allegations, IRR should ask themselves some questions to evaluate the information received and determine how to proceed.

For instance, the Office of Inspector General of the United States of America has created a table to inform potential whistle-blowers about the types of violations that can be reported, who can report and which institutions are the authorized recipients.[a] In this regard, upon receipt of allegations, initial recipients of reports must identify the category of whistle-blower, the type of information reported and whether the institutions that received the report are authorized to handle the allegations, in order to decide how to proceed further.

For example, civilian employees of the Department of Health and Human Services can report the following violations (exclusively):

- Violation of any law, rule or regulation
- Gross mismanagement
- Gross waste of funds
- Abuse of authority
- Substantial and specific danger to public health or safety
- Censorship related to scientific research or analysis (scientific integrity)

[a] Available at www.oig.hhs.gov/fraud/report-fraud/whistleblower.asp.

The following table contains a list of questions and actions that recipients of reports should take into consideration:[46]

QUESTIONS FOR INITIAL ASSESSMENT	POSSIBLE ACTIONS
What is the urgency of the report? • Is the alleged act of wrongdoing a one-off event, a recurring event or an anticipated event? • Is there harm to individuals? • Is there potential harm to a large portion of the population (e.g., production of altered drugs)?	All reports are to be handled in a timely manner. However, some reports might need to take priority when it comes to further handling (e.g., when there is immediate harm to individuals under medical treatment). In the health-care sector, it is important to evaluate to what extent the allegations could harm the health and well-being of individuals and how concrete and imminent those risks are.
Does the report include enough information to answer the other questions in this table?	If not, you will need to contact the whistle-blower and ask for more information. However, the whistle-blower cannot be asked to do investigative work. Communication with whistle-blowers should always be carried out with a high level of empathy. For safeguarding reasons, these communications should be carried out by someone who is professionally trained for this specific task.

(continued)

[46] The table is based on the table contained in UNODC, *Reporting Mechanisms in Sport*, and has been adapted for the purposes of the present study.

QUESTIONS FOR INITIAL ASSESSMENT	POSSIBLE ACTIONS
Is the reported wrongdoing under the jurisdiction of your organization? • Is the wrongdoing covered in the rules of the organization? • Does the organization have jurisdiction over the entity or individual mentioned in the report?	If the information reported is a criminal matter, you are required to alert the relevant authorities and hand over the matter to them. If further assessment is needed for these purposes, the report should be transmitted to the fact-finder. If it is not a matter of violation of a law, rule or policy but of dissatisfaction, and it will not be classified as another procedure or investigated, then this should be communicated to the whistle-blower, preferably in a conversation explaining why no further action can be taken. Written reasons for the decision should be provided. At this point, the whistle-blower might have further information. In any case, the report should be logged in the system. Depending on the reason for the dissatisfaction expressed by the reporting person, other more suitable procedures might be available in the organization, such as a grievance or management appeal procedure.
Have similar reports been made previously?	A report might not have enough information on its own, but when considered in parallel with information in other reports, a more viable case may appear. This is why it is important to log every report. Careful handling of allegations received requires you to review and track.
What are the risks of maintaining confidentiality? • Is the whistle-blower the only one who has access to the specific information? • Does the whistle-blower work in a small team?	The whistle-blower might have already spoken to someone about their concerns or they might be in a position where it is easy for others to guess who made the report. The employment history of a whistle-blower and the working relationship with the accused person(s) might be relevant to getting a proper understanding of the situation and potential risks. Investigators should be informed of these risks.
Has there already been retaliation against the whistle-blower?	If there has, the report may be influenced by anxiety and frustration relating to the reprisal. Communication with the whistle-blower is needed to separate the facts about the wrongdoing from those relating to the retaliation.

To answer some of the questions listed above, IRR (and, subsequently, investigators or fact-finders) may benefit from certain documentation and additional information. Whistle-blowers should be encouraged to give as much information as possible, but in certain circumstances, such as when anonymous reports are made, the information provided is limited and incomplete. Gathering more information can sometimes be essential to assess and investigate the alleged wrongdoing.

The following are examples of the types of documents and information that may be important, in some cases, in order for a report to be assessed and investigated:[a]

- Documentation regarding additional reports, such as a safety or health report or other statutorily protected report submitted to any other enforcement agency
- Copies of any relevant, lawfully obtained documents, such as emails, phone records, text messages, activity logs, meeting notes, work orders, letters or memoranda, related to the report
- Copies of any hiring and/or termination letters
- A copy of the employer's handbook for personnel and/or collective bargaining agreement
- Copies of any disciplinary action(s) taken against the whistle-blower during employment
- A current description of the whistle-blower's job
- Copies of the whistle-blower's last five pay stubs (if retaliation has already occurred and pay was affected)

[a] A similar list of helpful information to have when filing a complaint is available at: www.whistleblowers.gov/complaint_page.

In addition to the documents listed above, gathering a list of names and contact information of individuals who can verify the allegations could also be important. In this regard, whistle-blowers should be encouraged to identify the following persons:

- Potential witnesses who can confirm the allegations, including a brief summary of what each witness may know
- Management officials who made the decision that led to the alleged wrongdoing
- Individuals who processed the paperwork regarding the decision at issue (administrative, clerical or human resources personnel)

Most of the documents and contact information concerning such individuals might be in the organization's possession. Therefore, it is important to grant recipients of reports (as well as investigators or fact-finders) access to this information, so that the assessment of the allegations and the subsequent investigation can be carried out efficiently. In addition, document management systems for maintaining and preserving the security of information pertaining to individuals, disclosures and evidence must be utilized. Such documentation needs to be preserved adequately if it is to potentially inform criminal investigations.

Chapter 5.

CONDUCTING INVESTIGATIONS AND REVIEWS: FACT-FINDING

5.1 CARRYING OUT AN INVESTIGATION

When an organization establishes a policy to protect whistle-blowers, it is not only to build a culture of trust, but also to promote accountability, transparency and integrity. The organization may also wish to take a preventive approach and be informed about legal, administrative and disciplinary instances of wrongdoing committed within it, immediately investigate them internally and ensure that corrective actions are taken seriously and implemented swiftly.

In this regard, it is therefore essential to have a policy establishing how to handle internal administrative investigations. Since the term "investigation" can often be associated with criminal proceedings, another term, such as "administrative review", "management review" or "fact-finding", may be preferred in the policy.

There should be an office or a person in charge of gathering pertinent information to assess whether the allegations meet the relevant criteria. Some organizations have created a dedicated intake section. The persons in question must be duly trained to conduct such investigations, highly trusted (if possible, certified as examiners) and independent enough to undertake fact-finding in every investigation or review, including those concerning high-level or senior managers of the organization. Ideally, individuals performing the role should be outside the line management chain, so as to reduce the risk of interference in the process.

In some cases, especially in the public sector, units are created to both receive and investigate reports. In some instances, investigations are also outsourced. In such cases, extra attention must be paid to ensuring and maintaining the confidentiality of the information.

For instance, the Office of Investigations within the United States Office of Inspector General is in charge of receiving and reviewing allegations and, if warranted, assigning them for investigation. Sometimes, the allegations do not amount to whistle-blowing or require an investigation and are therefore referred to management as an inquiry requesting a response to the allegations.[a]

[a] For more information, see the website of the Office of Inspector General of the United States Department of State, available at www.stateoig.gov/hotline/whistleblower.

In other cases, in particular in the private sector, the receiving unit may be an external service provider while the investigator is within the company, usually in the compliance department, when such a department exists.

In some organizations, the fact-finder works within the compliance department of the organization, while the reporting channels are handled by an external provider. In this case, the external provider will transmit the information to the fact-finder after the initial assessment. When the information is deemed not to warrant an investigation, it is even possible that the initial recipients of reports might not provide the investigator with the name of the whistle-blower. Thus, nobody inside the organization has access to the identity of the whistle-blower.[a]

[a] Alternatively, an organization could outsource the investigation to an external provider.

Investigators might undertake the following activities:

- *Gather evidence of the alleged wrongdoing.* It is important that the investigator has unrestricted access to all documents and files of the organization. The confidentiality of documents cannot pose an obstacle to the investigation and, therefore, the policy should provide for the investigator to have immediate access to all documents, information, witnesses and persons under investigation (subjects). Moreover, sanctions can be imposed on those who refuse to grant access to potential evidence.[47]
- *Ask for further information from the reporting person, where necessary.* The investigator should obtain sufficient information to conduct an effective investigation.[48]
- *Conduct interviews and receive verbal testimony and written statements.* The investigator should be trained to understand the complexity of cases and ask the right questions. Many investigators are required to put the witness or subject under oath and record the interview.
- *Review the reported allegations(s)* and determine whether they involve potential fraud, corruption or any other illegal or criminal conduct warranting referral to national authorities, including law enforcement authorities as appropriate. Some investigations will involve untangling complex schemes and elaborate plans to avoid being detected. In these instances, investigators need to be sufficiently trained to detect them and obtain the evidence needed to prove that a crime may have been committed.
- *Formulate suggestions on recommended disciplinary and corrective actions.* When the investigation has concluded, the investigator will have to formulate a recommendation on what measures should be taken to address the wrongdoing that has been investigated and substantiated.

[47] See part two, sect. 5.2, of the present guidelines.

[48] See, for example, Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 9, para. 1 *(c)*.

5.2 CHOOSING THE IDEAL INDIVIDUAL TO PERFORM INVESTIGATIONS OR REVIEWS

The independence and impartiality of investigators is essential, especially when the investigation has not been outsourced. To help safeguard the role from adverse interference, the person in charge of internal investigations should not be tasked with additional job roles or functions. When not conducting investigations, this individual could participate in the continued development of the whistle-blower programme, training and awareness-raising. Where it is not possible to assign a person to a full-time role, the individual must have appropriate time allocated to them, away from their substantive role and responsibilities, to ensure that thorough and timely investigations are conducted. The investigator should not be put in a position that would result in rushed or incomplete investigations. It is necessary for the organization to establish a specific position of investigator or fact-finder and include this in its policy. There should also be a requirement that the individual selected for the position be familiar with the core business of the organization and obtain a recognized professional qualification concerning the conduct of criminal and/or administrative investigations, such as certification as a fraud examiner, within two years of taking up the position, if that person does not already have such a qualification.[49]

It may be possible for the organization to conduct an internal recruitment process. In such a case, the organization would then have to fund the certification.

However, the organization may consider it preferable to hire someone from outside. Indeed, it is possible that there may not be qualified personnel or that personnel may have conflicts of interest or even lack independence. The investigator will undertake fact-finding missions related to other personnel in the organization. If the individuals are recruited internally, they may not be perceived to be independent.

It may therefore be preferable to recruit an external candidate, so as to reduce the risk of investigations not being conducted in a completely neutral manner. In addition, by recruiting an external candidate, the organization can make appropriate qualifications a precondition for recruitment.

Whatever the case, the investigators or fact-finders must ensure their independence and must not be influenced in any way. They should be obliged to declare any conflicts of interests they might have that could potentially affect their impartiality. When an investigator or fact-finder declares a conflict of interest, it is advisable that the organization appoint another suitably qualified person to process the case.

Regarding the health-care sector, there might be strong opinions in favour of involving professionals such as doctors to assist in the investigation or review as programme experts. Since they will not need to be trained on the specific terms and procedures that they might encounter during the investigation, they can be used as specialists to assist in determining whether wrongdoing has occurred. Doctors or other health-care practitioners, especially those who have been working in the sector previously, might be familiar with some corrupt practices and, in some cases, could be of help to the entity or person responsible for conducting the investigation. Any time experts are brought into an investigation, it is recommended that they sign an independence or conflict-of-interest statement that includes express confidentiality provisions.

[49] For example, in some private companies, candidates selected to fill the post of investigator within the compliance department are required to be certified by the Association of Certified Fraud Examiners (www.acfe.com).

Chapter 6.

ADDRESSING THE WRONGDOING AND CLOSING THE CASE

To establish an effective policy on whistle-blower protection, it is not enough to receive allegations of possible wrongdoing. Actions must be taken to stop the wrongdoing, mitigate the consequences and enact sanctions against the persons who committed it.

It is worth noting that, in some cases, the process mentioned in part two, chapter 5 may lead to the conclusion that the allegations cannot be substantiated. The policy should therefore establish mechanisms to ensure that:

- The person (subject) against whom the allegations were made does not suffer any negative consequences. The confidentiality principle is also fundamental for this purpose.
- If damage to reputation or career has been caused, measures are established to repair or limit it.
- The whistle-blower is not subjected to retaliation or disciplinary action, provided that the person reported in good faith and/or on reasonable grounds.[50]

In some cases, before taking a final decision (including a decision to take no further action), the person in charge of assessing the alleged wrongdoing (initial recipient of report or investigator) can also be requested to consult with a superior or another colleague. In such situations, special care must be taken when consulting the person, in order to avoid jeopardizing the independence and impartiality of the final decision.

For instance, the Public Interest Disclosure (Whistleblower) Policy of the Australian Health Practitioner Regulation Agency provides that where a disclosure is being handled by a Public Interest Disclosure Officer, that Officer will consult with the Chief Public Interest Disclosure Officer before making any final decision on the disclosure (including a decision to take no further action).[a]

[a] www.ahpra.gov.au/about-ahpra/complaints/whistleblower-policy.aspx.

[50] See part one, sect. 2.3, of the present guidelines.

6.1 ADDRESSING THE WRONGDOING

If the investigation shows that the allegation of wrongdoing is true, or is very likely to be true, investigators should establish the nature of the wrongdoing in their report.

For cases where the instances of wrongdoing are non-criminal in nature, the policy should provide for a mechanism for taking and monitoring corrective actions. The report transmitted from the investigation unit to the organization's body in charge of disciplinary measures should include the identification of the type of wrongdoing and recommendations in terms of *(a)* enhanced internal controls and *(b)* disciplinary measures. In some organizations, disciplinary proceedings are handled by an external organization or an oversight body (such as the personnel board).

It is very important to maintain the confidentiality of the identity of the whistle-blower at every stage of the process, even if the subject of the investigation is going through a disciplinary process. If a disciplinary hearing is ultimately held and the whistle-blower is called as a witness, the identity of the whistle-blower should appear in the list of all persons who provided verbal statements during the investigation phase, without distinction.

The whistle-blower may still suffer some retaliation from colleagues or managers, even when the case is closed and the sanction has been imposed. In this case, some form of protection and/or compensation might be in order if the retaliation is proven.

In cases where the wrongdoing could also constitute a criminal offence – which would be the case if it were an act of corruption, for instance – the investigation unit must transfer the case to the competent prosecutor or law enforcement authority (if it does not itself have jurisdiction or authority to investigate). The policy should provide that in the event that an investigation uncovers a criminal offence, especially one with suspected links to organized crime (such as a network of corruption inside the organization), the investigator should stop its investigation and hand over the file to the competent authorities.

It is therefore essential that the policy contain the following instructions:

- When the case is criminal, or likely to involve a criminal offence, the file should be transmitted without delay to the competent authorities.
- The investigator, and the management of the organization, must remain at the disposal of the authorities for further investigations (it is important that the organization cooperates with the authorities).
- Whenever possible, the investigators should not initially communicate the identity of the whistle-blower to the competent authorities. However, in some cases, it could be essential for law enforcement authorities to know the name of the person who reported the case, including through judicial orders. Nevertheless, certain precautions must be taken, such as:
  - The whistle-blower must be informed and provide their express consent. The policy could contain a waiver form for this purpose.
  - The identity of the whistle-blower must be revealed in a confidential manner, and the policy should provide a mechanism for this.

It is important to note that, at this stage, if the country where the organization is located does not have whistle-blower protection legislation, taking the case outside the organization increases the risk of the identity of the whistle-blower being revealed, and the person could suffer retaliation. It is therefore highly recommended that the policy establish mechanisms to avoid having to provide the name of the whistle-blower (whenever possible). Another possibility is to conclude an agreement with the law enforcement authorities to authorize, for example, the investigator (or another person in contact with the whistle-blower) to play the role of an intermediary if more information must be collected.

6.2 CLOSING THE CASE

Additional aspects must be considered as the case is brought to a close.

First, a final report including all relevant legal or administrative violations, facts and evidence to prove or disprove the allegations and witnesses must be written. A release process must be followed, and the file must be secured after the case is closed. It is important always to remember that the whistle-blower may be subject to retaliation even after the process has ended. This is also true for cases in which it was concluded that no wrongdoing was committed and no corrective action was taken.

In this regard, is important to have clear guidance on the steps to follow, such as:

- Ensuring that, throughout all stages of the case, all processes have been carried out in accordance with planned and documented procedures and in compliance with legal requirements
- Ensuring that all decisions and actions have been logged in the case file
- Checking national requirements in relation to relevant laws on data protection in the country of operation. Data protection laws may require personal data in the case file to be removed or modified at this point. This is especially important in the health-care sector, since the files may contain medical information of patients and personnel
- Ensuring the strict confidentiality of the information relating to the investigation. Special care must be taken with regard to the technical and organizational measures needed to mitigate such risks and ensure data security
- Recording the date of closure and who made the decision to close the case
- Recording the file in line with existing data protection policies and internal record management practices (if available)
- Informing the whistle-blower about the closure of the case[51]

Second, the investigator could also suffer from retaliation. Internal investigators remain, in most cases, employees of the organization, and they might have been in touch with the reported person when making enquiries about the case. They may be under pressure to reveal the identity of the reporting person, drop an investigation or issue findings that are favourable to the alleged wrongdoer. As such, investigators could be at risk (depending on the reporting structure) if they resist interference from management or colleagues. It is also possible that they could ultimately become reporting persons themselves. A good policy should provide for the independence and safety that investigators need to carry out their work. They should always be protected from dismissal, demotion or discrimination linked to their participation in the investigation process.

[51] See, for example, Directive of the European Parliament and the of the Council on the protection of persons who report breaches of Union law, art. 11, para. 2 *(e)*.

Chapter 7.

PROVIDING PROTECTION TO WHISTLE-BLOWERS

Whistle-blowers may put themselves in a position of significant personal and professional risk.[52] By reporting instances of possible wrongdoing committed by their colleagues, peers or superiors, whistle-blowers expose themselves to the risk of retaliation in their work environment, which could take such forms as job loss, harassment, restrictions on conditions and access in the workplace or the reduction of responsibilities.[53] The lack of measures to protect against these forms of retaliation could diminish the impact of strong reporting channels. In other words, personnel will not come forward if they are unsure that protective measures will be put in place to minimize the risk they are taking.[54]

Protection against retaliation in the health-care sector is crucial. The sector accounts for a large share of gross domestic product (GDP) expenditure. The Organisation for Economic Co-operation and Development (OECD) has reported that "in 2019, before the onset of the coronavirus pandemic, average health spending as a share of GDP across the OECD was around 8.8 per cent. This figure has remained largely stable since 2009 as growth in health spending remained in line with overall economic growth since the last [2008] economic crisis."[55] Thus, health-care-related organizations are powerful, and individuals might think twice before reporting wrongdoing.

Moreover, it is important to note that a solid whistle-blower protection policy does not exclusively benefit whistle-blowers. Organizations will also benefit greatly. When in place, effective policies will encourage reports of wrongdoing that could prevent patient harm, major monetary loss or costly judicial or administrative sanctions, not to mention harm to an organization's reputation. For instance, early detection of fraud within an organization, and cooperation with law enforcement, could prevent criminal proceedings against the organization when such fraud is reported. It may also reduce financial damages caused by the illicit activity. After all, wrongdoing of any kind within an organization or against its personnel will have harmful effects on it. A robust whistle-blower protection scheme will help to support greater well-being and retention of personnel, thus leading to improvements in service delivery for patients and the public. The protection scheme should also be applicable to witnesses of the wrongdoing, colleagues of the whistle-blower

[52] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*.

[53] UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business*.

[54] For research on this topic, see Aled Jones, Annette Lankshear and Daniel Kelley, "Giving voice to quality and safety matters at board level: a qualitative study of the experiences of executive nurses working in England and Wales", *International Journal of Nursing Studies*, vol. 59 (2016).

[55] OECD Health Statistics 2020 database, available at http://oecd.org/els/health-systems/health-data.htm.

(including those who may be wrongly identified as the whistle-blower) and facilitators (including initial report recipients, investigators, managers and others tasked with handling whistle-blower reports).

Therefore, it is important that the organization, when establishing the whistle-blower policy, provides for protection against unjustified treatment. In this regard, the policy must contain:

- A definition of what is considered unjustified treatment in the organization
- Measures to prevent or stop retaliation
- Measures to sanction retaliation when it occurs

7.1 PROTECTION AGAINST UNJUSTIFIED TREATMENT

When the organization establishes a whistle-blower protection policy, it is important for it to determine the kinds of unjustified treatment from which the whistle-blower should be protected.

In this regard, in the United Nations policy on protection against retaliation, the term "retaliation" is defined as "any direct or indirect detrimental action that adversely affects the employment or working conditions of an individual, where such action has been recommended, threatened or taken for the purpose of punishing, intimidating or injuring an individual" as a result of the individual having reported misconduct, as set out in the policy.[56]

The organization must therefore define retaliation and provide a non-exhaustive list of retaliation scenarios in the context of the whistle-blower protection policy. Potential forms of unfair treatment or reprisal may include:

- Suspension, laying off, dismissal or termination of contract
- Coercion, intimidation, bullying or harassment, including sexual harassment
- Demotion or the loss of opportunity for promotion
- The transfer of duties or a change of location of work
- A reduction in wages or working hours
- The imposition or administration of any disciplinary measure, reprimand or other penalty, including those of a financial nature
- Discriminatory, disadvantaged or unfair treatment, including based on gender
- The threat of violence, damage to property or any other action that would result in injury or other crime
- Violence, damage to property or any other action that would result in injury or other crime
- Counter-allegations that are unfounded or untrue
- Blacklisting (a sector- or industry-wide agreement, whether formal or informal, that prevents an individual from finding alternative employment)
- The provision of inaccurate or untrue information in an employment reference to prevent an individual from obtaining future employment, or the refusal to provide a reference when requested to do so
- Prosecution under civil or criminal law for breach of secrecy, libel or defamation
- Any other unfair treatment or reprisal (threatened or actual) not otherwise covered by this list

[56] ST/SGB/2017/2/Rev.1, sect. 1.4.

For instance, the WHO policy on whistle-blowing and protection against retaliation defines retaliation as "a direct or indirect adverse administrative decision and/or action that is threatened, recommended or taken against an individual who has reported suspected wrongdoing that implies a significant risk to WHO or cooperated with a duly authorized audit or an investigation of a report of wrongdoing." The policy provides a list of actions that could constitute retaliation against whistle-blowers:

- Harassment
- Discrimination
- Unsubstantiated negative performance appraisals
- Unjustified contractual changes: termination, demotion, reassignment or transfer
- Unjustified modification of duties
- Unjustified non-authorization of holidays and other leave types;
- Malicious delays in authorizing travel, or the provision of entitlements
- Threat to the whistle-blower, their family and/or property, including threats that may come from outside WHO[a]

[a] WHO, "Whistleblowing and protection against retaliation".

The policy should therefore protect whistle-blowers from any form of retaliation linked to instances of wrongdoing that they report. Protection should also be afforded even when investigations later reveal that no wrongdoing has taken place, as long as the person had reasonable grounds to believe that the information was true at the time of the report.

It is worth noting that action taken against whistle-blowers must be assessed keeping in mind their contextual and situational realities. An action that could appear as normal from an external point of view may indeed be perceived as unjustified treatment, depending on various factors such as gender, class, race and other identities and/or vulnerabilities of the person in their social context. It is therefore essential not to have an exhaustive list and to allow for situations to be assessed on a case-by-case basis.[57]

It is also important to note that the most effective policies on whistle-blower protection do not limit the protection afforded to the whistle-blower *stricto sensu* (i.e., the first person who reports the wrongdoing), but extend it to all persons who cooperate in the whistle-blowing process, such as facilitators, witnesses, colleagues (including those wrongly identified as whistle-blowers) and family members who work at the organization.

7.2 MECHANISMS OF PROTECTION TO PREVENT OR STOP RETALIATION

When a country adopts a law on the protection of whistle-blowers, protection mechanisms are also created. The law may provide for the principle of confidentiality and the non-disclosure of the name and identity of the whistle-blower. To address cases in which the identity of the whistle-blower is revealed for any reason, and retaliation occurs as a result, the law may also establish mechanisms to either allow for compensation for damages caused (such as the possibility for the whistle-blower to take the case to the labour court or benefit from a reversal of the burden of proof) or stop the retaliation and reinstate the person in their functions or other equivalent functions.

When such a law exists, the organization wishing to establish a specific policy must be aware of the existing legal mechanisms and ensure that its policy complies with them.

[57] UNODC, *The Time is Now: Addressing the Gender Dimensions of Corruption* (Vienna, 2020).

For instance, the Republic of Korea has established the Anti-corruption and Civil Rights Commission, which has the authority to provide interim relief measures to whistle-blowers, such as requesting organizations to reinstate employees in their functions.[a] Any organizational policy should comply with the authority of the Commission when establishing their internal mechanisms to prevent the dismissal of whistle-blowers.

[a] Republic of Korea, Act on the prevention of corruption and the establishment and management of the Anti-corruption and Civil Rights Commission, art. 62-3.

However, when there is no law in place, or the law does not provide sufficient protection, the organization, when establishing the policy, still has a certain amount of flexibility to provide some level of protection to those members who decide to report wrongdoing using internal reporting channels.

Ensuring confidentiality

As mentioned in part two, chapter 6, it is essential that the policy provides for internal reporting channels that ensure absolute confidentiality and allow for the possibility of reporting anonymously. The fear of being discovered as a whistle-blower could involve more than concerns about losing employment. As shown in the example below, people might fear for their lives and the well-being of their families.

A study on whistle-blowers in the nursing sector contains the following statement made by a nurse upon being questioned about her initial feelings when she decided to blow the whistle: "There was probably a month or two where I was very concerned for my welfare or my children's welfare. I thought, even if he hasn't got the guts to come after me, maybe he'll go after my children. … There was a bit of concern there for a while."[a]

[a] Debra Jackson and others, "Understanding whistleblowing: qualitative insights from nurse whistleblowers", *Journal of Advanced Nursing*, vol. 66, No. 10 (October 2010), p. 2198.

Taking the case seriously and handling it promptly

Taking the case seriously and investigating it is essential not only to detect and address wrongdoing, but also to provide protection to the whistle-blower and prevent potential acts of retaliation. In fact, the more swiftly a case is handled, the lower the risk of the whistle-blower being identified or, if discovered, being retaliated against, as it would become clear that the retaliation is a consequence of the disclosure.

In addition, if whistle-blowers feel that reporting does not lead to any action, they may be discouraged from reporting in the future, lose confidence in the organization itself and consider going outside the organization to report (e.g., to the media). This is an important consideration in cases related to the health-care sector, as whistle-blowers resorting to the media or other external channels could lead to the violation of the rights of third parties through the disclosure of medical information or records.

In addition, some of the instances of wrongdoing committed represent a real danger to public health and people's lives. Whistle-blowers may therefore feel the urge to report publicly given the urgency of the situation. By protecting whistle-blowers, the organization also protects itself from potentially grave economic and reputational loss. The policy should emphasize the importance of reporting wrongdoing. Reporting breaches and wrongdoing can be a sensitive issue for cultural, legal and political reasons (e.g., whistle-blowers can be perceived as traitors or informants).[58] Providing protection to those persons includes changing this negative perception and encouraging more reporting.

[58] UNODC, *An Anti-Corruption Ethics and Compliance Programme for Business.*

Reassigning or reinstating the whistle-blower when necessary

The reassignment or reinstatement of the whistle-blower is an effective mechanism that could be put in place for the prevention and mitigation of the consequences of retaliation. In all cases, the reporting person should be consulted before possible reassignment or reinstatement, so that it is not perceived as detrimental treatment.

The policy will need to provide for the possibility of reassigning the whistle-blower to a new post, if the whistle-blower continues to work at the company after blowing the whistle. The relocation must not reduce the rank or salary of the whistle-blower.

> For instance, if the organization is large, the policy could offer the possibility for the whistle-blower to be moved permanently or temporarily to another department or branch, to avoid or stop retaliation from the original team.

For cases in which reassignment is not possible, the policy can also provide for other measures of relief, such as placement on special leave with full pay or any other appropriate action, including security measures, on a case-by-case basis.[59] Where reassignment is not possible, this should be made clear to the whistle-blower as soon as possible, in order to manage expectations.

The possibility of reinstating the whistle-blower to the job, if the person was dismissed before any protective measure could be put in place, should also be envisaged in the policy. Even when there is no national norm in place to reinstate the whistle-blower or repair the damage caused by retaliation, the organization could include internal mechanisms in this regard, depending on its size.

Such decisions must be taken after a proper investigation into the alleged retaliation has been conducted. A person or unit should be in charge of such matters. This person will typically be from the human resources department. The organization may also wish to consider providing the services of a mediator to re-establish working relationships between colleagues and a person accused of wrongdoing, in appropriate circumstances.

7.3 SANCTIONING AGAINST RETALIATION

Unfortunately, the measures in place to prevent retaliation are not always sufficient to effectively protect the whistle-blower. The policy must therefore include other mechanisms to sanction against retaliatory acts that may occur in the organization following a report.

Mechanisms to report and investigate retaliation

The policy must allow individuals to report unjustified treatment that arises following a disclosure. Therefore, the organization must specify in the policy that all established reporting channels for the disclosure of wrongdoing should also be able to receive complaints concerning retaliation or unjustified treatment that whistle-blowers may suffer after making a report.

It must be kept in mind that, when retaliation takes place, whistle-blowers and other staff might lose confidence in the reporting system. This is especially true when retaliation is a result of the revelation of their identity during the reporting process. In these cases, governmental organizations are also available to receive allegations concerning retaliation.[60]

[59] See, for instance, WHO, "Whistleblowing and protection against retaliation". In ST/SGB/2017/2/Rev.1, sect. 8.3, it is provided that the Ethics Office may recommend that the Secretary-General "take appropriate measures to safeguard the interests of the complainant, including, but not limited to, temporary suspension of the implementation of the action reported as retaliatory; with the consent of the complainant, temporary reassignment of the complainant and/or change of reporting lines; or, for staff members, placement of the complainant on special leave with full pay."

[60] For example, the Equal Employment Opportunity Commission of the United States is in charge of enforcing federal laws against discrimination against persons who have reported a discrimination situation.

The alleged retaliation (or unjustified treatment) must be investigated using the same mechanisms set out in the policy for the investigation of wrongdoing. It is, however, recommended that the person in charge of investigating the alleged wrongdoing not be also in charge of investigating the alleged retaliation. While connected, both processes must remain distinct and must be addressed independently of one another.

For instance, some medical supply companies provide for different reporting channels to report cases of retaliation. These may include the compliance officer, the ethics office and the human resources department, among others. In addition, as indicated in the present guidelines, several reporting channels should be established for reporting wrongdoing. Therefore, it is also possible for the whistle-blower to use a different channel to report allegations of retaliation from the one used to report the wrongdoing.

As mentioned above, retaliation can be defined as a direct or indirect adverse administrative decision and/or action that is threatened, recommended or taken against an individual.[61] In this regard, it can take many forms and also depends on the social, cultural, legal and political context of the organization or the country where an organization is located, as well as on the particular socioeconomic situation, gender and vulnerabilities of the reporting person. Therefore, a decision or action (such as a promotion or a transfer) that may be experienced or seen as normal in one country, in one organization or for one person, may be seen or experienced as unjustified treatment in another context. It is therefore necessary to link the alleged retaliatory act with an existing disclosure and place it in context in order to determine whether it is to be considered unjustified treatment.

Thus, retaliation involves three sequential elements:

- A disclosure concerning suspected or alleged reportable wrongdoing
- A direct or indirect adverse administrative decision and/or detrimental action or omission
- A causal relationship between the disclosure and the adverse decision and/or detrimental action or omission

In order to substantiate such an allegation, an investigation must find evidence of all three elements.

Ideally, the policy should provide for the reverse burden of proof, to the benefit of the whistle-blower. In other words, if the first two of the above-mentioned sequential elements are established by the investigators, the causal relationship will be presumed unless the person (or administration) suspected of retaliation can demonstrate through clear and convincing evidence that the act which is suspected to be retaliatory would have occurred even if the whistle-blower had not reported a suspicion of wrongdoing.[62]

Mechanisms to sanction against retaliation

Although sanctions are more common in legal instruments than in policies, organizations might benefit from the deterrent effect these could have among their personnel. For this to happen, all personnel will need to be aware of the sanctions that they could potentially face, and such sanctions should be aligned with existing disciplinary codes and policies.

When retaliation has happened and can be linked to the disclosure of wrongdoing, certain sanctions can be imposed on the retaliating person. Although some retaliatory actions could be seen as a violation of the code of ethics of the company and the perpetrator could be sanctioned on those grounds, it is important to regulate specifically the consequences of retaliation following a whistle-blower disclosure. This allows the company to establish proportionate sanctions and avoid very broad definitions that could result in the dismissal of the case.

[61] See, for instance, ST/SGB/2017/2/Rev.1, sect. 1.4, and WHO, "Whistleblowing and protection against retaliation".

[62] See, for instance, ST/SGB/2017/2/Rev.1, sect. 7.1, and WHO, "Whistleblowing and protection against retaliation".

For instance, codes of ethics might oblige personnel to behave in an ethical way without specifying the conduct that could violate this provision.[a] Although retaliation might be considered a violation of this obligation, it is left to the body in charge of disciplinary proceedings make that decision.

[a] For instance, in article 37, para. 2 of the Code of Medical Ethics of the Spanish General Council of Official Medical Associations, it is stated that "Physicians should treat each other with due deference, respect and loyalty, whatever the hierarchical relationship between them."

Retaliation in all its forms must be considered when drafting a list of sanctions. It is important to remember that conduct of a criminal nature must also be reported to the competent national authorities for investigation and, potentially, prosecution. Nevertheless, even when the wrongdoing is criminal in nature, the organization can impose disciplinary sanctions on the wrongdoer. In this regard, policies can provide for the imposition of the following sanctions, depending on the gravity of the wrongdoing:

- A warning or written censure to be retained in staff member's personal record
- Suspension without pay
- A reduction in pay or deferment, for a specified period, of eligibility for salary increment
- Demotion or deferment, for a specified period, of eligibility for consideration for promotion
- Reassignment
- Dismissal (with or without severance pay)

As disciplinary proceedings are not exclusive to whistle-blower protection policies, the body already in charge of such matters could take responsibility for the sanctions for retaliation. In most organizations, a specific and independent department within human resources should be responsible for analysing and deciding on sanctions.

7.4 PROVIDING SUPPORT AND FEEDBACK TO THE WHISTLE-BLOWER

It is suggested that the policy on whistle-blower protection also contain a procedure to provide *(a)* guidance and support to persons who would like to report alleged wrongdoing and *(b)* follow-up, on a regular basis, with the whistle-blower on the progress of the case.

Guidance and support

Reporting can be very stressful, especially for an employee of an organization wanting to report wrongdoing committed by colleagues, peers or superiors. The more a person knows about the procedure, the less hesitant they will be to report instances of wrongdoing and the more confident they will feel when doing so.

The initial recipient of report should be able to provide advice and support to the whistle-blower. As specialists in the whistle-blowing process, IRR can also help ensure that personnel who have knowledge of instances of wrongdoing trust them enough to report to them. As reporting may sometimes be cumbersome, owing to the amount and type of information needed, the processes that must be followed or the fear of exposure, for example, these experts should be receive training with respect to providing information to address any doubts of the potential reporting persons.[63] Whistle-blowers should also have access to an independent source of advice that is separate from IRR. This could be provided internally or be external to the organization.

Moreover, a specific person or office outside the official reporting mechanism might be designated or set up to provide information. For instance, a staff member might want to obtain information about the options

[63] See part three of the present guidelines.

available before making the decision to report. Compliance officers, an ombudsperson, a trusted supervisor, trade union representatives or employee representatives could play this role. Human resources departments are also traditionally designated to assist personnel, including by providing advice and support in this regard. In all cases, it is essential that designated persons are trained in providing advice and support to potential whistle-blowers with regard to sharing the information, and in dealing with whistle-blowing cases. Any new provisions should be aligned with existing arrangements and policies aimed at personnel well-being and support.

Special attention must be paid to the importance of confidentiality and anonymity in the reporting process. Information and technology resources, such as webinars, can be used to minimize the exposure and potential stigmatization of people who attend relevant events. The policy should ideally put in place a system whereby every person who is thinking of reporting can obtain confidential support and advice.

Support and advice can be provided on a non-personal basis. Websites and pamphlets can provide the necessary information.[64] The use of informative emails could also be an option. The General Medical Council of the United Kingdom has a dedicated web page explaining the type of information that can be reported to it and how to report other information. Moreover, it provides a guide entitled "Raising and acting on concerns about patient safety" that not only explains the steps to take to raise a concern but also lists useful contacts.[65]

In cases where the impact of the whistle-blowing disclosure results in a person needing to take time away from the workplace, organizations should consider all the options at their disposal to ensure that whistle-blowers feel able to return to work (if they wish to do so), for example by allowing personnel to take leave or work remotely. If possible, they should also provide access to an employer-funded support or counselling hotline.

Feedback

Once a report has been made, the whistle-blower may still deal with uncertainty, fear of retaliation or even fear that nothing will be done in response to the report.[66] It is essential that some follow-up is provided to reassure the whistle-blower that the disclosed information has been taken seriously. As mentioned above, the first step in this follow-up should be the acknowledgement of the receipt of the report, if it was made remotely, for example through email, a mobile application or the Internet.[67]

Providing too much information about the case to the whistle-blower could jeopardize the investigation or the disciplinary process. Therefore, the policy should state that the whistle-blower will be kept informed about the general progress of the case, without prejudice to any confidential aspects of the investigations that may be conducted. Where possible, estimated time frames should be provided. The person in charge of this process should always act in an appropriate manner and in line with the training that should have been provided.

If it is concluded through the initial assessment or the investigation that no further action needs to be taken, the whistle-blower should be informed promptly about this decision. It is advisable to thank the individual for coming forward, even if the concern will not be acted upon. This helps to support an open whistle-blowing culture.

[64] For instance, WHO developed a simplified version of its policy on whistle-blowing and protection against retaliation, in the form of a short brochure, which provides key information on who can report, what can be reported, how to report and what protection can be afforded to reporting persons. The brochure is available at www.who.int/about/ethics/whistleblowing-and-protection-against-retaliation.

[65] See General Medical Council of the United Kingdom, "What concerns should you raise with us?" and "Raising and acting on concerns about patient safety", available at www.gmc-uk.org.

[66] UNODC, *Reporting Mechanisms in Sport*.

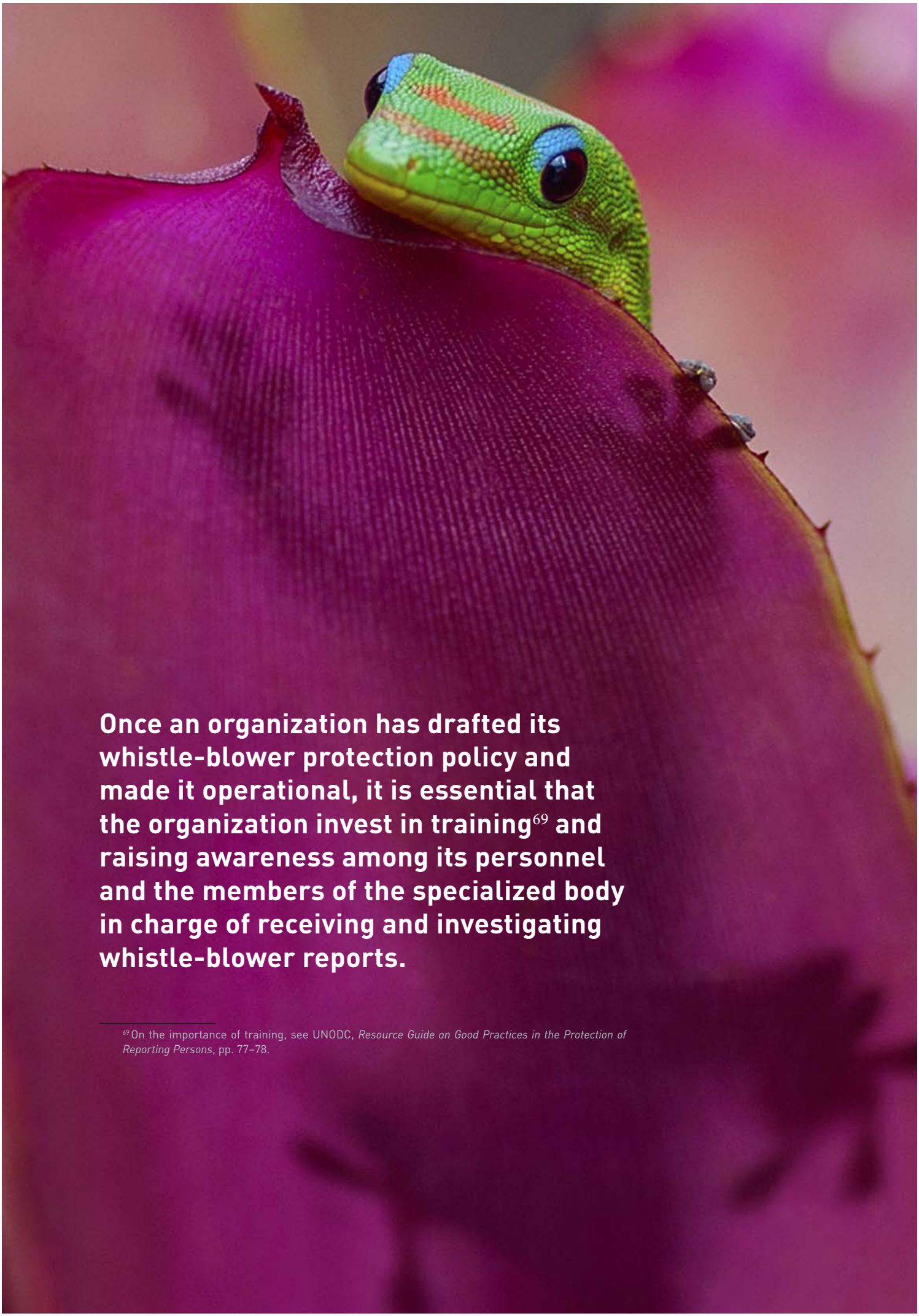
[67] See part two, chap. 4, of the present guidelines.

The policy must contain a timeline for providing support and feedback to the whistle-blower. For example, the European Union directive provides for a time frame not exceeding three months.[68] The whistle-blower should also be informed about what they will and will not be entitled to know during the process and when the case is brought to a close, in order to manage expectations. This is necessary to build a culture of trust and confidence in the organization. If the person does not feel listened to or taken seriously, or if they feel that the report did not lead to any action, they may take the case outside the organization and make it public. Such a lack of confidence in the system could also spread, creating an environment that discourages the reporting of wrongdoing.

[68] See Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 9, para. 1 *(f)*.

PART THREE

TRAINING AND RAISING AWARENESS



Once an organization has drafted its whistle-blower protection policy and made it operational, it is essential that the organization invest in training[69] and raising awareness among its personnel and the members of the specialized body in charge of receiving and investigating whistle-blower reports.

[69] On the importance of training, see UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*, pp. 77–78.

Chapter 8.

TRAINING INITIAL RECIPIENTS OF REPORTS, INVESTIGATORS AND PERSONNEL

As mentioned above, the establishment of a whistle-blower protection policy and procedure requires the organization to hire staff (or identify existing personnel) with the knowledge, the skills and the ability to assess whistle-blower allegations and conduct investigations. Moreover, everyone involved in the whistle-blowing process must receive appropriate training to ensure that reports are handled properly, with care and in accordance with national law.

8.1 TRAINING INITIAL RECIPIENTS OF REPORTS

It is important for the initial recipients of reports (IRR) to be trained to handle the reports and to be aware that they are required to grant protection to whistle-blowers.[70] As confidentiality is essential in the protection of whistle-blowers, when a person discloses an alleged instance of legal or administrative wrongdoing, IRR should treat the information provided with care. It has been documented that, in some societies, the information provided varies depending on the appearance of the person to whom the wrongdoing is being reported; cultural and societal norms should also be taken into consideration.[71] IRR should be trained and sensitized to receive and handle reports that may be delicate or distressing and to be understanding of the needs and vulnerabilities of female whistle-blowers or whistle-blowers from minority groups.[72] The role of IRR also involves a certain amount of outreach to establish trust and thereby encourage reporting from all members of the organization. In the health-care sector, it is important for IRR to be familiar with the terminology and procedures used in their organizations.

In view of the products, services and amounts of money involved in the health-care sector, it is not uncommon for reports to constitute evidence of crimes of corruption or against the public well-being. Where possible, IRR should have some form of legal training. At a minimum, IRR should be trained to identify when a disclosure could constitute a criminal offence. IRR would therefore benefit from training concerning the most common crimes committed in the sector, such as pharmaceutical fraud or corruption in the

[70] On the importance of training the person in charge of receiving and following up on reports, see Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law, art. 12.

[71] Nicolas Hamelin, Mehdi el Boukhari and Sonny Nwankwo, "Micro-credit, gender and corruption: are women the future of development?", in *Women and Social Change in North Africa: What Counts as Revolutionary?*, Doris H. Gray and Nadia Sonneveld, eds. (Cambridge, United Kingdom, Cambridge University Press, 2018).

[72] Zúñiga, "Gender sensitivity in corruption reporting and whistleblowing".

health-care sector, and common crimes committed in the workplace, such as embezzlement. When a potential crime is identified, IRR must, with supervisor approval, inform the relevant law enforcement authorities.

In addition, IRR are responsible for informing whistle-blowers about the whistle-blowing procedure, procedural guarantees (i.e., confidentiality, prohibition against retaliation and the right to be informed about the status of the report, among others) and protective measures.

IRR must also be trained to take into account the contextual and social realities of reporting persons and demonstrate sensitivity and responsiveness in their work. They must consider individual factors, such as the reporting person's belonging to a marginalized or vulnerable social group and the intersectionality of the different aspects of the person's identity, such as race, class and gender. Accordingly, IRR should receive specialized training on gender and diversity issues.

8.2 TRAINING INVESTIGATORS

Training should also be provided to investigators or fact-finders. Some of the training provided to IRR, such as how to handle reports or the terminology and procedures used in the organization, could also be useful to investigators. However, training of fact-finders must be focused on enhancing their investigative skills.[73] In this context, and to facilitate the professional development of fact-finders, the organization should invest in formal training courses and certification to conduct internal investigations, including financial investigations. Historical analyses of cases in the sector and in the organization could help them understand where to look for vulnerabilities, red flags, potential gaps and sources of each instance of wrongdoing. The organization should maintain official records in the form of secure archives to facilitate the learning process.

Investigators should be trained on the procedures and sanctions provided for in the organization's whistle-blower protection policy, as investigators are in charge of drafting the recommendations at the end of the investigation setting out the sanctions to be imposed, if any, for the alleged wrongdoing or retaliation.

Finally, as with IRR, investigators must demonstrate a high level of sensitivity and responsiveness in their duties. Therefore, they should receive gender and diversity training to enable them to take into account the individual situation of each whistle-blower in their investigations of alleged wrongdoing or retaliatory acts.

8.3 TRAINING ALL PERSONNEL

The organization should endeavour to provide appropriate and adequate training to all personnel on the whistle-blower protection policies, mechanisms, remedies and support available to them.[74] Such training should be incorporated into induction programmes. In addition, training should be provided to relevant departments, such as human resources, compliance and monitoring and the office of the ombudsperson, on how to treat or process allegations and how to guide and support individuals who have reported or are considering reporting wrongdoing. The organization should also ensure that upper management, senior managers and supervisors are trained to provide appropriate guidance to personnel, including on how to treat or process allegations and reports. It is also recommended that the organization consider using electronic and online tools such as e-platforms and e-learning resources to conduct such training. Training should be provided at regular intervals to ensure ongoing learning and the training materials should be updated frequently to ensure that they remain relevant and reflect applicable laws and best practices. The organization should endeavour to evaluate learning outcomes so as to measure the effectiveness of the training.

[73] An example of a training programme for whistle-blower complaint investigators is the mandatory programme for whistle-blower investigation personnel, see United States Department of Labor, Occupational Safety and Health Administration (OSHA), "Mandatory training program for OSHA whistleblower investigators", Directive No. TED-01-00-020, 8 October 2015.

[74] See UNODC, *An Anti-corruption Ethics and Compliance Programme for Business*, pp. 69–72, and United Kingdom, Department for Business Innovation and Skills, "Whistleblowing: guidance for employers and code of practice" (London, 2015), p. 5.

To summarize, the organization should provide the following categories of training:

- Training of IRR on how to respond, what questions to ask, what advice to give, which actions to take and how to maintain confidentiality
- Training of investigators or fact-finders on how to conduct investigations
- Training of personnel in relevant departments (e.g., compliance, office of the ombudsperson) to provide support to and follow-up with whistle-blowers
- Training of management and senior managers on receiving reports, providing guidance to personnel and forwarding the disclosure to the relevant person or unit in charge of fact-finding
- Training of all personnel on whistle-blowing rights and remedies, available guidance and existing mechanisms.

Chapter 9.

RAISING AWARENESS

Organizations should combat the culture of silence that may exist among their personnel by raising awareness of the benefits of whistle-blowing. Without a whistle-blowing mechanism in place, the downsides of reporting misconduct can be all too obvious to personnel and may deter them from speaking up. An effective whistle-blower protection policy must promote an environment that supports and welcomes open criticism, dialogue and discussion.[75]

Whistle-blowing can be presented as an opportunity to reflect on and improve the quality of care, rather than as an act that is damaging to individuals.[76] Health-care practitioners often feel a calling to help others and the organization should help them perceive reporting as an opportunity to improve the health-care system. The goal should be to change how those who decide to report malpractices are perceived.

However, it would be naive to think that all personnel will step up and disclose potential wrongdoing solely out of a sense of duty. The organization needs to set the tone at the top and make ethical principles, integrity and zero-tolerance part of the organizational culture.

In order to raise awareness among all personnel, it is crucial that everyone has access to information. The organization should make the whistle-blower protection policy publicly available to all persons who may be in a position to raise concerns, not only employees. All personnel should be informed and reminded on a regular basis, through posters in meeting rooms and tailored communication and training activities of the existence and content of the policy.

The following questions should be answered:

- Is there an internal whistle-blower protection policy?
- Why should I report my concerns?
- What misconduct can I report?
- Whom should I report my concerns to and how?

[75] Jackson and others, "Understanding whistleblowing", citing Benisa Berry, "Organizational culture: a framework and strategies for facilitating employee whistleblowing", *Employee Responsibilities and Rights Journal*, vol. 16 (March 2004), pp. 1–11.

[76] Ibid.

- Will my name, identity and information be kept confidential if I submit a report?
- What risks do I face?
- If I decide to report, what protective measures will be put in place?

This information should be advertised or marketed using a variety of means, such as pamphlets, flyers, brochures,[77] posters and, depending on the size of the organization, talks, role-play training and seminars could be held to inform personnel about the different mechanisms, channels and protection measures available. The organization may also choose to publicize its policies on its intranet, through a regular newsletter and request the assistance of the relevant staff unions to ensure greater dissemination.

[77] See, for instance, WHO, "Whistleblowing and protection against retaliation".

Chapter 10.

LEARNING FROM THE PROCESS: RISK ASSESSMENT

Organizations can enhance internal controls by tracking findings, recommendations and corrective actions from closed cases. By maintaining and analysing the data, organizations can detect patterns, which can be an important learning tool for the organizations concerned, within and outside the health-care sector. The development of knowledge bases can help guide future whistle-blowing mechanisms and aid in the development of new corruption mitigation strategies for the health-care sector. Knowledge bases are also a crucial tool for raising awareness and breaking the taboo and the dilemmas associated with whistle-blowing. Learning from closed cases may help to:

- Improve reporting interfaces
- Conduct initial assessments
- Reduce organizational risks
- Classify reports
- Innovate investigative processes
- Improve communication

Keeping track of closed cases also helps to build a foundation of good practices that may be adapted and implemented in the future. For example, the Virginia Mason Medical Center in Seattle, United States, uses data obtained through a "Patient safety alert system" to improve its safety culture.[78] Another essential and effective practice involves keeping the formal records of all reports and investigations undertaken at the organizational level, irrespective of the outcome or result.

Such records can serve as an analytical tool for mapping out potential risk areas and patterns within the organization in order to include and focus on them in regular risk assessments. This in turn facilitates the development of tailor-made mitigation measures for particular risk areas. The organization may therefore wish to adopt or improve its policy on record keeping and record management.[79]

[78] For analysis, see Aled Jones, "The role of employee whistleblowing and raising concerns in an organizational learning culture: elusive and laudable? Comment on "Cultures of silence and cultures of voice: the role of whistleblowing in healthcare organisations", *International Journal of Health Policy and Management*, vol. 5, No. 1 (January 2016).

[79] See UNODC, *State of Integrity: A Guide on Conducting Corruption Risk Assessments in Public Organizations* (Vienna, 2020).

One way to adopt and strengthen mitigation measures for a particular risk area is to engage in a corruption risk assessment process.

The goal of the risk assessment process is to identify a realistic set of potential risks, prioritize them and develop and implement efficient, cost-effective mitigation measures and strategies. Findings, recommendations and corrective actions from past cases initiated by internal reports can be a precious source of information at all stages of the process.

Once an organization has committed to conducting a corruption risk assessment, the first step is to conduct an internal self-assessment. Such an assessment consists of reflecting on the external and internal factors that shape the behaviour of the organization and its members, the powers the organization has over those factors and constraints it faces in exercising those powers. Any existing laws and regulations and internal whistle-blower protection policies and procedures should be included in the self-assessment. The personal and professional integrity of personnel, the management's philosophy and style, the way the organization reacts to reports and information from closed cases will provide an insight into relevant external or internal factors and demonstrate how the organization has operated when presented with a particular risk of corruption.

The second step is to identify potential corruption risks. The corrupt practices or potential corruption risks evident from closed cases may be included in the list of identified corruption vulnerabilities to inform the risk assessment process. Once the list is established, the organization should analyse it and use it as a basis for conducting interviews with staff, examining internal documents, past findings and recommendations and reviewing existing corruption controls.

The third step is to assess potential corruption risks according to the likelihood that they will occur and the severity of their impact. Two of the key questions that should be asked to estimate the likelihood of a corruption risk are whether similar acts of corruption have occurred in the organization or similar organizations and whether internal procedures include sufficient safeguards to deter those who would want to commit such acts. The information provided by reporting persons and the information included in the closed cases are very relevant in this regard.

It has been demonstrated that when individuals are asked to estimate risks, they tend to overestimate or underestimate the likelihood of some events depending on their familiarity with them. Organizations can counter familiarity bias by asking individuals why they think that one act of corruption is more likely to occur than another, or whether recent cases may have affected their estimates. Information included in closed cases or reports may or may not be indicative of the likelihood of a risk being a factor again, depending on the context and the facts of a particular case.

If both the likelihood and the impact of a particular corruption risk are high, the risk should be prioritized, and a relevant mitigation strategy should be developed. In order to do so, the organization must analyse existing controls, including its procedures, rules and measures aimed at preventing and detecting corruption. Once again, previous findings, recommendations and corrective actions can help identify existing controls that may not be effective, determine why they are not effective and what kind of new controls may be needed. As organizations have limited resources, the new controls must be feasible and affordable if they are to be effective. In order to be realistic, the new controls should be specific, clear and their cost should not outweigh the potential loss associated with a particular corruption risk. Once new mitigation measures have been identified, they should be incorporated into the organization's operational and strategic workplans, implemented and regularly reviewed and evaluated.

However, it is crucial that the principle of confidentiality be carefully observed in the context of the corruption risk assessment process. Indeed, while data extracted from closed cases represent a precious source of information, the types and kinds of data extracted must be reviewed so as to not inadvertently reveal, hint at or lead to the identity of the reporting person (such as the reporting person's office number or department). However, such information may have already been revealed if such exposure had been previously authorized by law, for example, if the explicit consent of the reporting person had been obtained. Although the case is closed, the risk of retaliation might still exist. Therefore, it is essential that the group in charge of

conducting the risk assessment work in close collaboration with the person or the unit in charge of whistle-blowing investigations to assess the level of information they can be given access to and what information can be reflected in the risk assessment table. In all cases, information procured from closed cases must be cross-checked in order to ascertain the principle of confidentiality.

The corruption risk assessment process is detailed in the UNODC publication *State of Integrity: A Guide on Conducting Corruption Risk Assessments in Public Organizations*, which provides further information and may be a useful reference for organizations that wish to use the lessons learned from closed cases to mitigate and prevent future corruption risks.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 263-3389, www.unodc.org

V.21-01920