ICC Guidelines on Whistleblowing 2021

I. Introduction

The purpose of these Guidelines is to help Enterprises establish and implement a Whistleblowing Management System, by offering practical guidance that will serve as a useful point of reference. The original ICC Guidelines on Whistleblowing were published in 2008 and this update incorporates current experience and practice of ICC member Enterprises across a wide range of sectors and jurisdictions worldwide. They have been aligned with key international legal instruments as well as global standards and best practice for Whistleblowing Management Systems[1].

Whistleblowing is the act of reporting a Wrongdoing. Unaddressed, such harm can erode the trust of the stakeholders in the Enterprise's governance and can destroy the Enterprise's shareholder value.

Employees of an Enterprise and those in close contact with them (including Business Partners and other Third Parties) are often the first to recognize a potential Wrongdoing or risk of harm. They are therefore valuable sources of information and well placed to support resolving a potential problem early on before it causes material damage to the Enterprise and the society.

It is therefore in the interest of a responsible Enterprise to encourage Whistleblowing as part of its Ethics & Compliance Programme, or its ethics guidance, and to set up a system to support Whistleblowing. A well-functioning and trusted Whistleblowing Management System supports Enterprises' ambitions for sound risk management, internal control and effective compliance, and promotes a culture of transparency, integrity and accountability.

While the term "Whistleblower" can awaken different feelings in different countries, it has today become an internationally recognized term to denote persons who report suspected or actual Wrongdoings. Therefore, Whistleblowing can in a corporate context range from raising concerns, speaking up or submitting a confidential report via an Enterprises' Whistleblowing channel.

Enterprises today are, among other criteria, measured by how they deal with Whistleblowers and how well they handle reports and concerns that are brought to their attention. The ICC Rules on Combating Corruption recommend that Corporate Compliance Programmes adopted by Enterprises offer "confidential channels to raise, in full confidentiality, concerns, seek advice or report in good faith established or soundly suspected violations without fear of retaliation or of discriminatory or disciplinary action".

II. Whistleblowing Management System

Whistleblowing Management System means the Enterprise's programme, objectives, mechanisms, channels, policies and processes relating to Whistleblowing. The purpose of a Whistleblowing Management System is to enable reporting through organized communication channels set out by the Enterprise to ensure that concerns of Wrongdoing swiftly reach those that are most able to investigate the matter and empowered to remedy it.

Prior to introducing a Whistleblowing Management System, the Enterprise must ensure that the system it intends to use complies with applicable laws and regulations of the countries in which the Enterprise operates. In particular, local laws on data transfer, data protection and privacy as well as

[1] The definitions in this document are based on the ISO 37002:2021, Whistleblowing management systems — Guidelines and the ICC Business Integrity Compendium.

local labour laws and specific Whistleblower protection regulation must be assessed. Note that certain legal instruments set out specific requirements regarding the organisation of an Enterprise's Whistleblowing Management System.

The cultural environment in which the Whistleblowing Management System will operate, the organizational model of the Enterprise and the governance of the Enterprise will determine how the Enterprise's Whistleblowing Management System should be arranged within the Enterprise.

As confidentiality is the foundation of a trustworthy Whistleblowing Management System, it must be designed to ensure that the Whistleblower's identity as well as the identity of the accused and any other sensitive information disclosed in the Whistleblower report, are not disclosed to anyone beyond the personnel designated to receive or follow up on reports. This should not preclude disclosing information in a protected form when legally required.

Each individual Enterprise will have to decide, bearing in mind the laws of the countries in which the Whistleblowing Management System will operate as well as its corporate governance, whether:

- reporting under the System will be compulsory or voluntary,
- reporting will be incentivised e.g., by offering a reward to the Whistleblower,
- reporting and investigation of reports will be centralized or de-centralized,
- whether anonymous reporting will be allowed or not, and
- reporting by third parties and/or general public will be enabled.

A well-managed Whistleblowing Management System is easy and safe to use and is embedded in the governance of the Enterprise.

Enterprises should provide a list of persons and bodies to whom Whistleblowers can raise concerns depending on the circumstances and location. The reporting channels for Whistleblowing should accommodate different preferences, accessibility and abilities of potential Whistleblowers with possibilities for both oral and written reporting, such as telephone-based reporting (toll free call helplines or hotlines), digital reporting (e-mail or webform), by writing a letter to the designated person or any other tool which is fit for Whistleblowing or for reporting in person directly to the responsible staff. Enterprises should endeavour to make reporting channels available in multiple languages, depending on the countries of operations, and create awareness of these reporting channels in the Enterprise's normal tools for communication. Clear and accessible information is key to promote uptake of the channels.

III. Scope

A Whistleblowing Management System should be designed to receive and handle reports about Wrongdoing, whether actual or potential, established or reasonably suspected.

Wrongdoing includes action(s) or omission(s) or concealment of an act or omission that can cause harm. In a narrow sense it relates to breach of national or international law or legal obligations, fraud or corruption. In its broadest sense it includes misconduct of whatever kind in the context of the workplace, such as, but not limited to, conflicts of interest, risk of harm to human rights, the environment or health and safety, harassment or discrimination in the workplace, or other breach of the code of conduct or the code of ethics, or any other integrity standard, of the Enterprise.

When planning the Whistleblowing Management System, the Enterprise should define its expectations of what the Whistleblowing Management System should seek to achieve, what type of

reports of Wrongdoing it wants to have in a centrally managed channel, and which are the alternative channels for reporting, the resources and the qualifications required for receiving and managing reports, how the Whistleblowing Managing System will be embedded in the Enterprise's overall governance and how the Enterprise will communicate about the System.

The Whistleblowing Management System should be made available to the Enterprise's directors, officers and employees, its trainees, interns and volunteers as well as other persons working under the supervision or direction of the Enterprise in the countries where the Enterprise operates. Enterprises should consider opening their Whistleblowing channels to persons working under the supervision or direction of their Business Partners and Third Parties, and if relevant, also beyond their circle of third parties to include potential Whistleblowers in the society at large. However, before enabling external parties to use the Whistleblowing channels of the Enterprise, the Enterprise must consider whether and how protection can be afforded to such extended category of Whistleblowers.

The Enterprise should further consider whether the Whistleblowing channels should be limited to reports of Wrongdoing or can also be used for asking questions or consult on compliance issues and/or alert the Enterprise to general risks of danger to health, safety or the environment. Note that a Whistleblowing Management System is generally not suitable for dealing with emergencies.

IV. Non-retaliation

It is paramount for the trust in the Whistleblowing Management System that the Enterprise does not tolerate any form of retaliation. A prohibition on retaliation should be included in each Enterprise's Code of Conduct or other relevant Integrity Standard or Policy.

Retaliation means any direct or indirect punishment, retribution or disadvantage (or any threat of such action) - which is prompted by internal or external reporting - to the Whistleblower or the legal entity that the Whistleblower owns, works for, or is otherwise connected with in a work-related context or to any person related to the Whistleblower, which might be of concern to the Whistleblower. In particular, the safety, the future employment, remuneration and career opportunities of the Whistleblower must not be impeded by the act of reporting.

Retaliation can include - and the Whistleblower should therefore be safeguarded against - dismissal, suspension, disciplinary action, coercion, intimidation, harassment, discrimination, blacklisting, business boycotting, early termination or cancellation of a contract, withholding of payment, license or permit, loss of business or income, denial of training, ostracism, blocking access to resources, re-assignment or relocation, demotion or any other harm or victimization to be caused or threatened as a consequence of actual or suspected Whistleblowing.

It can also be necessary at times to extend the protection against retaliation to persons who have facilitated or supported the Whistleblower or the investigation such as witnesses, colleagues or relatives. Where retaliation takes place by a third party or other external parties, the Enterprise must seek to do whatever it can within its area of influence to protect the Whistleblower from retaliation.

If a Whistleblower commits an offence or is complicit in an offence, or if the report is found to be knowingly false, the Whistleblower cannot expect Whistleblower protection or to be immune from disciplinary sanctions. It should, however, be abundantly clear that the sanction is not a form of retaliation but a consequence of the offence committed.

V. Roles and responsibilities

The recipient and investigator of Whistleblowing reports must be trustworthy. Therefore, in designating persons in charge of receiving and handling Whistleblowing reports it is advisable to carefully consider criteria of impartiality, seniority, reputation, competence and expertise as well as inclusion and diversity. These personnel should be given a large degree of autonomy and should report to the highest echelon possible within the Enterprise.

Enterprises are encouraged to develop competence in-house and build capacity for receiving and handling Whistleblowing reports. In cases where Whistleblowing reports are channelled outside the internal Whistleblowing Management System, Enterprises must ensure the confidentiality, completeness and security of such external channels. Such person or firm should be impartial and of unblemished reputation and should instil comfort of professionalism, confidentiality, experience and competence in handling and protecting sensitive and personal data.

Enterprises shall ensure that, where a report is received through internal channels other than the designated reporting channels or by personnel other than those responsible for handling reports, the personnel who receive the report are prohibited from disclosing the content of the report and any information that might identify the Whistleblower or the person concerned, and that they promptly forward the report without modification to the personnel responsible for handling reports.

Commissioning periodic audits of the effectiveness of the Whistleblowing Management System as well as establishing independent oversight of the Whistleblowing process by the Board, the Audit or Risk Committee or equivalent body or external advisors should be considered where possible, as these are valuable mechanisms for achieving assurance in the working of the Enterprise's Whistleblowing Management System.

VI. Awareness and communication

A Whistleblowing Management System cannot work in isolation but must form part of continuous efforts to build a strong foundation of ethics and integrity that encourages employees to speak up and voice any concerns. The promotion of the Whistleblowing Management System must reach all employees of the Enterprise and must explain why whistleblowing is encouraged, how it should be done and when. The educational effort should also bring transparency with regards to the process and foster a sense of organisational justice by explaining what will happen when a report is received, and that retaliation will not be tolerated.

It is equally important to educate managers and the personnel who receive reports on how to listen and create psychological safety for those who come forward and on how to handle the information they receive, including data protection provisions and confidentiality. It should be recognized that submission of a confidential report via the Enterprise's Whistleblowing channel is often seen as a last resort when employees do not feel encouraged to report their concerns directly to their manager. Therefore, Enterprises should clarify in their internal communication how to differentiate between "a report" and the mere information about an issue that requires management attention and needs to be rectified in the normal course of business.

While the Whistleblower should not be expected to provide evidence of the Wrongdoing, they should be educated to make the report genuinely, diligently and with reasonable grounds in light of the circumstances and the information available to the Whistleblower at the time of reporting. It should also be made clear that Whistleblowers who do not meet such standard are contributing to an environment of mistrust if it is found that the System is open for misuse.

Reporting through the Whistleblowing System should always be the recommended route before reporting to external channels (e.g., competent authorities) or releasing it in the public domain (e.g., in social media). The rights of the Whistleblower to report externally, e.g., to relevant competent authorities, must be made transparent by the Enterprise from the outset and pursuant to applicable data protection and data privacy rules.

VII. Management of the report

Any Whistleblowing report must be timely and diligently acknowledged (typically within seven days), recorded, triaged, and investigated or otherwise addressed, under strict confidentiality rules (on a need-to-know basis) by an appropriate competent person, department or unit.

The designated person, department or unit may be the same as the one who received the report. However, decisions about disciplinary actions or remedial measures related to the persons involved in the Wrongdoing should involve appropriate managers and the Human Resources department in accordance with local laws and the governance of the Enterprise.

While it is normally not advisable to convey details of the investigation or its findings to the Whistleblower, the steps that have been taken should be appropriately communicated as feedback to the Whistleblower within a reasonable timeframe (typically within three months).

The person whose behaviour has been reported should also be informed of the main object of the report, unless such information would pose a threat to the Whistleblower, be considered detrimental to the investigation, or prohibited by law. In any case, and to the extent permitted by law, this person's presumption of innocence and rights of defence, hearing and access to the file shall be respected while maintaining the confidentiality of the Whistleblower and any witnesses. The person, department or unit in charge of the investigation should determine, on a case-by-case basis, when and how the report and its investigation should be communicated.

Enterprises should maintain, to the fullest extent possible and at all times, the confidentiality of the data revealed through the Whistleblowing System, and the identity of the Whistleblower and any witnesses, subject to overriding legal requirements, and should protect such data with the most appropriate means and technology pursuant to any applicable data privacy rules. No data or report should be kept longer than necessary and proportionate to comply with applicable laws and regulations.

Whistleblower reports must be recorded and the investigation, including minutes of meetings, should be adequately documented and kept in a retrievable form. The records should not be stored longer than necessary according to the purpose they were collected, and according to local laws and requirements set out by the Enterprise's auditors.

Enterprises are encouraged to publish general statistics about Whistleblowing and key performance indicators in its communication channels to provide comfort to employees and stakeholders that reports are taken seriously and are professionally handled, and that the Enterprise seeks to improve on ethical behaviour at all times.