CEP Magazine - December 2021
It's time to assess your reporting and investigations protocols

By Rebecca Walker, Esq.

Rebecca Walker (rwalker@kaplanwalker.com) is a partner in the law firm of Kaplan & Walker LLP, based in Santa Monica, California, and Princeton, New Jersey, USA.

Reporting and investigations systems are critically important components of a compliance and ethics program. Indeed, according to the U.S. Department of Justice and the Securities and Exchange Commission, "The truest measure of an effective compliance program is how it responds to misconduct."[1] Whether an organization's response to misconduct is the *truest measure* of an effective compliance program is subject to debate. However, it is beyond doubt that robust systems to encourage reporting and to investigate allegations are essential to an effective program. They are also highly probative of a company's commitment to compliance.

The European Union (EU) Directive 2019/1937 (Whistleblower Directive), which is required to be transposed into national law by EU member states by December 17, 2021, highlights not just the importance of protecting whistleblowers from retaliation, but also places a spotlight on robust reporting and investigations. For any organization, these developments present an excellent opportunity to review reporting and investigations procedures, consider relevant standards and best practices, and make appropriate enhancements.

The EU Whistleblower Directive

The Whistleblower Directive on the protection of persons who report breaches of Union law, which was adopted by the European Parliament on October 7, 2019, applies to all companies that operate in the EU with 50 or more employees (and to municipalities that serve 10,000 or more people). Companies with 250 or more employees must comply with the directive beginning December 17, 2021. Businesses with between 50 and 249 workers have two additional years, with a deadline of December 17, 2023, for compliance.

The directive provides protection against retaliation for those who report alleged violations of EU law in a work-related context, including current, former, and prospective employees; contractors; unpaid trainees; volunteers; and even those who facilitated reporting, such as colleagues and relatives. This protection includes requirements (1) for companies to create internal reporting channels and (2) regarding how companies must respond to reports received. The directive encourages internal reporting, providing that member states "shall encourage reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation."[2]

The directive is focused on reports of violations of EU law and specifies those categories of violations that must be within the scope of protection. They include public procurement, financial services, anti-money laundering and terrorist financing, product safety, transport safety, environmental protection, food safety, privacy, cybersecurity, and other topics.

While the directive sets out minimal standards for member states, it also expressly provides that member states can adopt more rigorous whistleblower protections.

The directive's requirements for reporting procedures

In furtherance of its goal of protecting reporters, the directive includes a number of requirements related to reporting procedures for those companies to which the laws will apply.

Confidentiality

First, internal reporting procedures must include channels for receiving reports that are designed, established, and operated in a manner that ensures that the identities of the reporting person and any third party mentioned in the report are protected and that prevents access by nonauthorized employees. While confidentiality has always been a linchpin of effective reporting systems, these new requirements present an important opportunity for companies to revisit their means of protecting the confidentiality of reports received and investigations conducted. This will likely include both assessment of case management systems and training relevant personnel on the importance and means of protecting confidentiality.

Avenues and records of reports received

The Whistleblower Directive requires that companies permit reports to be made in writing, orally, or both, with oral reporting avenues via telephone; voice messaging systems; and, upon request by the reporting person, a physical meeting within a reasonable time frame. Companies are further required to keep records of every report received, although the record keeping must be in compliance with confidentiality requirements, and records may be stored for no longer than necessary and proportionate to comply with the requirements imposed by the directive or other EU or national law. The Whistleblower Directive also contains specific rules for how calls may be documented (e.g., through a recording or a complete and accurate transcript, in which case the reporting person must be offered the opportunity to review, modify, and agree to the transcript by signing it).

Similarly, where a person reports by way of an in-person meeting, the company is required, subject to the consent of the reporting person, to create and maintain a complete and accurate record of the meeting in a durable and retrievable form. The record may be made by recording the conversation or through accurate minutes of the meeting, and again, the reporting person must be offered an opportunity to review, modify, and agree to a written record of the meeting by signing.

For these requirements, companies should communicate with their helpline providers to ensure compliance with record-keeping obligations. In addition, companies should implement protocols to ensure that, when they receive reports directly, the reports are either recorded or minutes of meetings are maintained, and that the reporting person is given the opportunity to review the record of the meeting.

Acknowledgment of receipt

The Whistleblower Directive requires that companies acknowledge receipt of the report to the reporting person within seven days. It further requires that companies provide feedback to the reporting person within a reasonable time frame, not exceeding three months from the acknowledgment of receipt. Acknowledgment and feedback are important because they enhance employee confidence that their concerns are being appropriately addressed by the company. It is therefore helpful for any company to include acknowledgement and feedback in their reporting and investigations protocols.

Designation of appropriate personnel

The directive also discusses the designation of an impartial person or department competent for following up on

the reports. This provides organizations with an opportunity to consider how reports are triaged and assigned for follow-up, and also to consider the background, expertise, and training of the company's investigative resources.

Anonymous reporting

European countries have historically been reluctant to allow employees to report concerns anonymously, although that aversion has eased over time. The Whistleblower Directive allows member states to decide whether to permit anonymous reporting.

Reporting outside the company

The Whistleblower Directive also requires member states to establish external channels for employees to report suspected violations of EU law, which must include the designation of competent authorities to receive, give feedback to, and follow up on reports. The agencies must be provided with adequate resources to receive and handle reports. The directive requires that companies provide clear and easily accessible information regarding the procedures for reporting externally to competent authorities. This information will likely need to be added to appropriate communications to employees for affected organizations.

An opportunity to assess and improve

The Whistleblower Directive's requirements create an important opportunity for organizations to assess and improve their reporting and investigations processes. Those companies that are subject to the directive should begin by assessing their current reporting and investigations systems against the requirements of the directive and of local law, which may vary in different member states. At minimum (and, really, regardless of whether a company is subject to the directive), it is critically important to ensure the implementation of secure and confidential reporting channels and to designate appropriate personnel to receive, assign, and investigate reports. Companies should also adopt and publicize strong anti-retaliation policies. Companies should consider reviewing existing (or, if they don't already have them, creating) reporting and investigations protocols to ensure that the various requirements of the directive will be satisfied. Such protocols also help ensure consistent responses to reports received and protect the integrity of reporting and investigations systems.

Just to complicate matters a bit more, companies operating in the EU are, of course, still subject to data protection laws and regulations, and it is important to ensure that reporting and investigations systems are compliant with those laws also.

Companies that are subject to the directive should train those employees who handle reports and investigations on the new requirements and should consider conducting training and communicating to all employees the importance of reporting suspected misconduct, the reporting avenues available, and the nonretaliation policy.

A good time to review

How an organization responds to reports of suspected misconduct is an important element of a compliance program and a critical measure of the culture of compliance. The Whistleblower Directive creates a slew of new obligations for affected companies, but it also creates an important opportunity for organizations to review and enhance their reporting and investigations systems. Indeed, regardless of whether the Whistleblower Directive is applicable, this is an ideal time for any company to improve these elements of their compliance programs.

Takeaways

- The European Union's Whistleblower Directive, EU Directive 2019/1937, provides an important opportunity for companies to review reporting and investigations procedures, consider standards and best practices, and make appropriate enhancements.
- Confidentiality has always been a linchpin of effective reporting systems.
- The directive requires that companies acknowledge receipt to the reporting person within seven days.
- European countries have historically been reluctant to allow employees to report concerns anonymously. The directive allows them to decide whether to permit anonymous reporting.
- It is critically important to ensure the implementation of secure and confidential reporting channels and to designate appropriate personnel to receive, assign, and investigate reports.

1 Department of Justice and Securities and Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, July 2020, 67, https://www.justice.gov/criminal-fraud/file/1292051/download.
2 EU Directive 2019/1937, O.J. L305, Art. 7(2), https://bit.ly/3BDakob.