Whistleblowing â€“ A Guide to Compliance: Part 3

Crowell & Moring LLP's 2021 series of client alerts: Whistleblowing – A Guide to Compliance is intended to provide companies with a practical guide to help them comply with their obligations under the EU Whistleblower Directive. Via a monthly alert, Crowell & Moring LLP will explain the different steps that companies need to take for compliance and emphasize various points for consideration.

STEP #3: Understanding the obligations of (U.S.) companies with operations in various EU member states

As mentioned in our Alert #1, the EU Whistleblower Directive should be transposed by the EU member states into national law by December 17, 2021. This same deadline applies to the obligation of companies to establish their internal channels and procedures in accordance with the EU Whistleblower Directive and the relevant national law (although there is a possibility to provide for a later deadline of December 17, 2023 for private companies with 50 to 249 workers).

National implementation by the EU member states will not result in full harmonization, and whistleblower legislation will likely differ in the individual EU member states. The EU Whistleblower Directive provides only minimum standard provisions and EU member states are allowed to introduce certain provisions that are more favorable to whistleblowers (e.g., by extending the material scope of the legislation to cover breaches of national law). The EU Whistleblower Directive also leaves certain aspects to the discretion of the individual member states (e.g., whether to accept and follow up on anonymous reports, and as regards the sanctions that can be imposed).

The deadline of December 17, 2021 is fast approaching, and we recommend that companies already start putting internal reporting channels in place, based on the provisions of the EU Whistleblower Directive. Companies with operations in various EU member states will need to keep monitoring the relevant national implementation and adjust their procedures to take local differences into account.

And this is not all. In addition to the above, U.S. multi-national companies will likely want to have a whistleblower procedure in place that complies with both the EU Whistleblower Directive and U.S. Regulations – and this can be tricky.

U.S. companies operating in any EU Member States should begin to take steps now to comply with this EU Whistleblower Directive, taking into consideration several open questions that will be

resolved as EU Member States incorporate the directive into their own national legislation, as well as the possibility that some states may offer greater protections to whistleblowers. U.S. companies with operations in the EU should therefore closely monitor national member state implementation in order to evaluate their existing channels, procedures and policies for compliance.

What should a whistleblower reporting program include?

Article 9.1: Internal reporting channels. Companies must establish secure channels and procedures for internal reporting and follow-ups. The EU Whistleblower Directive allows companies some discretion in establishing their own internal reporting channels. Options include: an ombudsperson, creating an e-mail account to receive whistleblowing reports, or contracting with an external vendor that provides digital whistleblowing platforms. Each type of reporting channel has its own risks, which must be evaluated before settling on a policy. For example, an e-mail-based reporting system may be easier to set up and use, but there are significant EU privacy risks to consider.

Recital 34: Anonymous reporting. The EU Whistleblower Directive does not address whether anonymous reporting is acceptable; this has been left up to the EU member states. U.S. companies should look to the law of the country in which they are operating and review its national legislation incorporating the EU Whistleblower Directive. It is likely that if a country previously allowed anonymous reporting, it will continue to do so.

Article 9.1 and Recital 56: Designation of an impartial person or department to investigate reports. This person or department's role is to receive any whistleblowing reports, follow up with the whistleblower, and if necessary, follow-up for further information. The investigator should be independent and free of conflicts of interest. Companies may designate an internal department, such as Human Resources or the legal department to receive and investigate reports. Alternatively, a company may want to use a third-party vendor, such as an external platform provider. A smaller company in particular may find an external vendor the most useful given that its internal Human Resources or legal departments may already be spread thin.

The designated person or department must acknowledge receipt of a report within seven days and provide feedback to the whistleblower within three months, unless it would prejudice the investigation or affect the rights of any implicated individuals.

Recital 59: Notice. Companies must inform their employees, as well as other persons that may come into contact with the company (e.g. distributors, suppliers, and business partners) of the company's internal reporting procedures and external reporting procedures (e.g. reporting to the government). Such notice may be provided through posters at visible locations on the worksite, the company's website, or in trainings on ethics and integrity. While training is not required, the best practice would be to conduct a company-wide training once the whistleblower policy is in place.

Articles 16.1-16.2: Confidentiality is key. Only the persons or departments designated to receive and follow-up on reports should have access to investigation reports, whistleblower complaints, and documents revealing the identity of the whistleblower. This should be explicitly laid out in the company's policy and adhered to in a strict manner. For example, should the company wish for its CEO to be informed on a "need-to-know" basis of any reports or the outcome of an investigation, this should be explicitly stated in the policy.

Confidentiality is also important for compliance with the EU's data privacy policy, the General Data Protection Regulation ("GDPR"). An updated whistleblower policy should reflect key GDPR requirements: (1) personal data (such as the identity of the whistleblower) cannot be kept longer than necessary; (2) appropriate safeguards must be used if personal data is transferred outside of the European Economic Area; and (3) the subject of the whistleblower's report may have a right to access the file, subject to anonymization or removal of any third-party's personal information.

Recitals 87; Articles 6, 7.2: Retaliation will not be tolerated. Company policy should make it explicit that retaliation against a whistleblower is against the law. Retaliation includes termination of employment, demotion, change of duties or place of work, a negative performance review, any other disciplinary measure, harassment or ostracism, failure to renew a temporary employment contract, harm to a person's reputation, or blacklisting. An employee has the right to report internally through the employer's own channels, externally to government authorities, or through public disclosure. Though the EU Whistleblower Directive encourages the use of internal channels first (unless the employee faces a risk of retaliation), companies cannot discipline employees who use external channels, as long as the employee had reasonable grounds to believe the matters reported upon were true.

Conclusion

The EU Whistleblower Directive is part of a global rise in whistleblowing—both in the number of whistleblowers and the strength of whistleblower protection laws. In 2020, the SEC hit a record high number for its whistleblower claims that were processed and the number of awards made to whistleblowers. The number of whistleblower claims received by the Office of Inspector General for the Small Business Administration is at an unprecedented high. California now authorizes its courts to award attorneys' fees to a plaintiff who prevails as a whistleblower and lengthens the

period of time in which employees can file complaints.

In the Asia-Pacific region, traditionally not protective of whistleblowers, multiple countries have introduced whistleblower protection laws recently. In Japan, large companies that do not properly establish a reporting system may be subject to administrative action, and employees who unjustifiably disclose the identity of a whistleblower may be fined. Australian companies that fail to have a compliant whistleblowing policy now may be fined up to $125,000 AUD.

The global rise in whistleblower protections does not stop there. In 2018, the United Arab Emirates passed a law prohibiting retaliation against employees who make good faith disclosures of failures to comply with applicable laws. Mexico, in 2016 alone, enacted four new laws and amended multiple existing pieces of regulation that, among other things, require companies to establish robust whistleblower reporting systems. Following up on its 2013 anti-corruption law, Brazil enacted a new law in 2018 authorizing all 26 of its states to create whistleblower hotlines and offer rewards for reporting and investigation.

Not only are robust reporting programs necessary to comply with whistleblower protection laws, but promoting channels for whistleblowers to report concerns and thoroughly investigating those concerns benefit the company as a whole. The purpose of the EU Whistleblower Directive is to "[lay] down common minimum standards providing for a high level of protection of persons reporting breaches of [EU] law." Many of the procedures required by the EU Whistleblower Directive are likely to make investigations more efficient, less likely to result in legal proceedings and, ultimately, beneficial to the health of the company and its employees.

Action point #3:

Start implementing internal reporting channels in place, based on the provisions of the EU Whistleblower Directive.
Monitor the different EU member states' national implementation of the EU Whistleblower Directive to identify specific national requirements.

Emmanuel Plasschaert
Partner – Brussels
Phone: +32.2.282.4084
Email: eplasschaert@crowell.com

Stefanie Tack
Counsel – Brussels
Phone: +32.2.282.1848
Email: stack@crowell.com