

Operationalizing the EU's New Whistleblower Directive Amidst the Global Pandemic

NOVEMBER 2020

By Julia Arbery

Like all EU Member States, Germany must translate the new EU Directive for Whistleblower Protection ("Directive") into national law by 17 December 2021. This legislation presents a significant change for companies operating in Germany and throughout the EU, as they will now need to thoroughly evaluate and enhance their existing compliance program and modify policies and procedures to ensure that heightened standards on protecting whistleblowers, responding to whistleblower complaints and maintaining safe and anonymous reporting channels are being met.

The ongoing global pandemic is likely to further complicate a company's ability to comply with the new protection standards. Companies in Germany should expect an uptick in whistleblower claims related both directly and indirectly to COVID-19, as well as to emerging environmental, social and corporate governance (ESG) risks such as Fridays for Future and the Black Lives Matter movements. Should a "second wave" of coronavirus outbreak take hold, nascent whistleblower protection protocols will quickly be pressure-tested by claims related to employee safety issues and fraud. Now more than ever, companies must foster a Speak Up culture and ensure that leaders are actively listening and taking swift and appropriate action in order to mitigate devastating reputational, regulatory and legal risks. But how can German organizations do so with reduced personal contact and limited in-person supervisory oversight?



Julia Arbery

Managing Director,
StoneTurn

jarbery@stoneturn.com
+49 (0) 69 710 455 457

To help companies get started, we provide an overview of the minimum standards set by the new Directive in the EU as well as best practices for companies and compliance professionals to consider as they navigate and implement these new standards amidst easing COVID-19 lockdown orders, GDPR constraints and local employment laws.

Required Level of Protection

Under the new Directive, companies with more than 50 employees are obliged to implement a whistleblowing procedure to handle disclosures of alleged wrongdoing within the organization. Yet, according to a study of Germany companies by Transparency International, “internal whistleblowing policies are not very common in Germany’s private sector and can typically only be found in big corporations. Even there they often lack independent addressees, involvement of staff, feedback to and rights for whistleblowers and transparency of their application.”

While many companies will provide for the opportunity of raising a concern internally, confidentially or anonymously, as well as protection against retaliation, best practice is to go a step further to offer “clear and safe” internal reporting channels. This includes an often overlooked means for the whistleblower to report retaliation related to his/her disclosure. Establishing a channel for the whistleblower to “close the loop” in this manner becomes increasingly important as in-person monitoring of retaliation-seekers is less feasible given pandemic-related work and travel constraints. In addition, HR and leadership must be sensitized to the risk of retaliation. For these reasons, an independent party to support the whistleblower

during and after the investigation process is recommended.

Keep in mind however, that companies must balance the requirements around confidentiality of internal investigations, transparency obligations and data subject access rights under General Data Protection Regulation (GDPR). This will require a case-by-case review and can be very tricky, especially as case law and experience with both GDPR and future legislation implementing the Directive is still extremely limited.

Effectiveness of the Internal Reporting Procedure

According to the new Directive requirements, there must be clear reporting channels both internally within the organization and externally to public authorities that ensure the confidentiality of the whistleblower and any third parties mentioned in the report and prevent access to nonauthorized employees. A clear and easy-to-follow and accessible procedure is crucial in encouraging employees to report wrongdoing. But practicality must also be considered. For example, a recent study of companies in the nearby Netherlands found that a majority of companies (66%) offer whistleblowers an in-person reporting option. Given current remote working conditions for most in the EU as well as the possibility of future COVID-19 outbreaks forcing work from home, in-person reporting mechanisms are far less effective. Instead, any outlet for reporting should be accessible remotely in order to allow for confidentiality and also available 24/7 to allow for time differences.

Employees should also be guaranteed a sufficient level of information, security and objectivity throughout all stages of the process. Based on the EU Whistleblower Protection Directive, companies must provide those who report wrongdoing with a follow-up within three months, the maximum timeframe for a follow-up. However, a 90-day lapse in communication can easily give rise to secondary claims and/or calls to media or another outlet. Companies should ideally respond within 7–14 days to acknowledge receipt of the claim and then provide an update on the resulting investigation within 30 days. Further, in cases where a subject access request has been received to identify the whistleblower, a thorough evaluation of all interests involved need to be weighed against each other and documented accordingly.

Supportiveness of the Corporate Culture

As part of the new Directive, companies are required to provide a written or electronic statement of the whistleblower reporting procedure to all employees. Best practices that will be well-received by regulators include:

- Efforts to build awareness of the reporting mechanism
- Training employees, leadership and supporting functions on the use of system
- Proactive reporting to management on the outcomes of whistleblower claims as well as to employees in an appropriate (anonymized/ aggregated) manner

Frequently assessing the effectiveness of the reporting system, including testing the reporting

Regulators expect companies to look beyond the numbers and act when prompted by statistics that reveal hot spots for potential issues.

channels, will also help reinforce a supportive corporate culture. While most companies do perform annual reviews of their whistleblower protocols and compliance performance metrics—will this frequency be deemed sufficient by a regulator if whistleblowers were not adequately protected? Further, is any sort of qualitative assessment of the data taking place? Regulators expect companies to look beyond the numbers and act when prompted by statistics that reveal hot spots for potential issues. Similarly, Compliance and HR leaders must be prepared to delve deeper if there is a prolonged lack of claims or consistently low level of whistleblower reports, as this could be an indicator of mistrust.

Last, the Directive requires that employees who report misconduct are protected against retaliation. This means that in cases of alleged retaliation against whistleblowers, employers will have to prove they are not punishing whistleblowers for speaking up, rather than the burden of proof lying on the employee. Effective protection of whistleblowers against retaliation may include Compliance working together with leadership and HR to implement specific procedures aimed at their protection.

Conclusion

With fraud and misconduct expected to increase as the result of the coronavirus crisis and new whistleblower protection legislation looming, it's never been more critical for companies in Germany and across the EU to revisit their compliance programs and whistleblower protections. The good news is that the same best practices that ensure compliance with the new Directive, also enable members of a remote workforce to safely and easily flag early warning signs of a potential issue, before they become larger problems down the line.



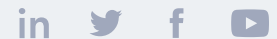
This article was initially published in **Compliance Management Magazine, Issue 24**. All rights reserved.

About the Author

Julia Arbery, a Managing Director with StoneTurn, has more than 15 years of experience in ethics and compliance. She assists multinational corporations with the development and implementation of effective ethics and compliance programs and specializes in the establishment of whistleblower frameworks and investigative protocols that comply with global data privacy and protection regulations.

Leaving no stone unturned.

StoneTurn, a global advisory firm, assists companies, their counsel and government agencies on regulatory, risk and compliance issues, investigations and business disputes. We serve our clients from offices across the U.S., U.K. and in Germany, Brazil and South Africa, assisted by a network of senior advisers around the world.



[StoneTurn.com](https://www.stoneturn.com)