Germany's Shifting Risk and Compliance Landscape

OCTOBER 2021

Julia Arbery
Partner, StoneTurn
jarbery@stoneturn.com
+49 1756838679

By Julia Arbery

Although the country's landmark "Law to Strengthen Business Integrity" ("Gesetz zur Stärkung der Integrität in der Wirtschaft") stalled at the end of the legislative period prior to the 2021 elections in late September, compliance teams and management must stay focused on upcoming requirements that will impact businesses operating in Germany. For example, should the new administration not implement local legislation adopting the minimum standards of the EU Directive on Whistleblower Protection, the Directive will be applied directly after December 17. Similarly, legislators recently adopted the Supply Chain Due Diligence Act ("SDDA"), requiring companies based in Germany with 3,000 or more employees (1,000 employees by 2024) to minimize human rights-related and environmental risks along their supply chains. These latest requirements, combined with current regulations, raise the compliance stakes for companies operating in Germany. But as the pandemic enters its second year and economic uncertainty abounds, are compliance practitioners truly prepared to meet continuously heightened local—as well as supranational—requirements and regulator expectations?

What Business and Compliance Leaders in Germany Have to Say

Last year, BCM's 7th annual occupational field study assessed compliance through the lens of business leadership and helped highlight the challenges that compliance practitioners in Germany/Austria and Switzerland are currently facing.

Specifically, although business leaders consistently view compliance practitioners as senior-level educators, consultants and translators of legal requirements, the compliance function's direct impact on the organization lags behind. Only 53% of 2020 respondents indicated that the advice provided by compliance is factually reflected in organizational policy and only 43% viewed compliance as being involved by specialist departments at an early stage. Perhaps most concerning is the apparent gap between what executives perceive as Compliance's remit and what practitioners actually view as their day-to-day responsibilities, with the leadership of internal investigations a particularly troubling disconnect. Not surprisingly, marks for the Compliance team were higher in organizations where digitization was more advanced and/or where compliance practitioners were able to demonstrate ROI to leadership.

Clearly, the 2020 survey results do not bode well for the success of government-imposed directives with no demonstrable ROI other than the avoidance of steep penalties. It will be interesting to compare these metrics with the results from BCM's soon-to-be-revealed 8th annual, 2021 occupational study. Still, given that government regulators acting under the auspices of either the whistleblower directive, SDDA or long-standing Administrative Offense Act will scrutinize an organization's investigative procedures, what is the likelihood that the average German company will qualify for leniency?

Understanding the Pending EU Whistleblower Directive

Like all EU member states, Germany must translate the new EU Directive for Whistleblower Protection into national law by 17 December 2021. If the deadline is missed the minimum standards will apply directly. Despite the complications arising from the pandemic in terms of reduced resources and remote work, companies operating in Germany must thoroughly evaluate and enhance their existing whistleblowing programs 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.

Specifically, under the EU 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 German companies by Transparency International, "internal whistleblowing policies are not very common in the private sector and can typically only be found in big multinational corporations. Even there they often lack independent addressees, involvement of staff, feedback to and rights for whistleblowers and transparency of their application."

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 non-authorized employees. Any disclosure must be balanced with the requirements around confidentiality of internal investigations, transparency obligations and data subject access rights under General Data Protection Regulation (GDPR) and will likely require a case-by-case review since relevant case law and experience with both GDPR and future legislation implementing the Directive is yet to come.

The Directive further specifies that those who report wrongdoing must be protected against retaliation, as well as provided with follow-up communications. Both internal and external reports must be acknowledged within seven days of receipt, and a response must be issued within a reasonable amount of time—three months for internal reports and up to six months for more complex external reports. However, one can easily see how even a 'compliant' 90- or 180-day lapse in communication can give rise to secondary claims and/or calls to media or another outlet – such as the highly popular and increasingly global Securities and Exchange Commission's (SEC) Whistleblower Hotline. Other requirements of the whistleblowing directive should be easier to meet prior to year-end, such as providing a written or electronic statement of the whistleblower reporting procedure to all employees.

However, the ongoing global pandemic is likely to further complicate a company's ability to comply with the new protection standards overall. Companies in Germany should expect an uptick in whistleblower claims related both directly and indirectly to COVID-19 which could quickly pressure-test nascent internal reporting mechanisms and budget-constrained internal investigation resources. Further, Germany's 4G mobile network is one of the worst in Europe. Cash still accounts for 75% of transactions. Few stores allow card payments on amounts under €10. And during the height of the COVID-19 pandemic, health authorities had to fax in their updates to Berlin, with home-schooling and remote-working handicapped by the same lack of computers and absence of high-speed Internet. Given this, are new technology-based reporting and tracking tools likely to be embraced and highly utilized by the average worker? If not, can in-person reporting be relied upon as an adequate first line of defense in an increasingly remote and global work environment?

Toplining Corporate Accountability in Germany Today

Currently, German authorities address corporate misconduct through the Administrative Offense Act 1968 (Ordnungswidrigkeitsgesetz or OWiG). Companies can be held liable if a representative of the company commits a criminal or administrative offense (see Section 30 OWiG), the result of which is a violation of the company's incumbent duties, or where the company has been enriched or was intended to be enriched. No criminal sanctions apply. Administrative fines may amount to €10 million if the representative committed a criminal offense with intent and €5 million if the representative committed a criminal offense negligently. In the case of an administrative offense, the administrative fine for the company is capped at the maximum fine for the individual multiplied by a factor of 10. In addition to the fine, any profit gained by the offense can be disgorged.

Under the recently adopted SDDA, regulatory fines can be levied for non-compliance of up to 2% of the annual global turnover in Germany, a potentially significant sanction. However, German courts may be less aggressive given the lack of clarity in some of the infringements defined in the SDDA.

The German SDDA defines protected legal positions and human rights-related and environmental risks on the basis of 14 international conventions listed in an Annex to the SDDA. Companies must take "adequate measures" to prevent or mitigate human rights-related and environmental risks related to these criteria. Further, regulated companies must perform due diligence with regard to their own business (including group companies), and their direct suppliers. When it comes to indirect suppliers, regulated companies may have to take action if there is sufficient evidence of human rights or environmental risks, no matter how far along the supply chain. But what constitutes "adequate measures" and "sufficient evidence"? And with more corporate third parties engaging with fourth, fifth and sixth parties and global supply chains generally in flux – where will regulators draw the line in terms of accountability?

Conversely, the German SDDA is quite prescriptive regarding the "cure"—specifically, a risk-based approach and the establishment of a risk management system, including regular risk assessments, the adoption of preventive measures / controls, reporting obligations and/or the establishment of a complaint mechanism. This is of particular concern given that small- and mid-sized German companies are less likely to have well-established compliance structures. But clearly, the SDDA, EU Whistleblower Directive and even the 50+-year old OWiG suggest that a robust compliance framework must be made a priority.

What Matters Most to Regulators

At an exclusive panel discussion convened by global advisory firm StoneTurn and business law firm Comfield Legal, German regulators pinpointed their priorities for 2021 and beyond. Their guidance provides important clues as to where compliance practitioners should focus their efforts amidst a changing regulatory environment.

1. **It Starts at the Top:** At its core, compliance is a management issue. Too often, management leaves compliance to the legal or compliance team and does not take an active role in the process. Prosecutors take this into account, with the decisive factor the company culture in practice. You can have the best rules, but they must be followed.

   Compliance must be "embedded" into the organization so that employees don't have to think about how to obtain the information they need. "Tone from the Top" sounds more difficult than it is. The central point is to set an example. The compliance department merely coordinates and checks to ensure protocols are being followed. In this period of increased M&A, the onboarding of smaller companies (e.g., sales units) is especially critical, because they often come with little compliance structure.

2. **Utilize a Risk-Based Approach** In the absence of clear guidance from German regulators, business leaders may be tempted to implement generic, 'check the box' compliance processes and procedures. Instead, management should view compliance as an opportunity to enrich the organization with a more risk-based approach. The business' specific risk profile and risk appetite should be assessed, with custom internal controls put in place to address both without being cumbersome. After all, when a prosecutor analyzes where misconduct has occurred, the question quickly becomes if it could have been avoided. Risks must be the subject of regular discussions with leadership as they evolve constantly. It helps to have input from specialist departments—such as accounting, sales, and purchasing—to gain a more representative and holistic view. This will be viewed favorably by the prosecutor.

3. **Leverage Technology:** While there is some debate over which tasks should be digitized in the compliance world, there is great value in many of the technology-based tools at the disposal of compliance practitioners. Companies can use these tools to monitor (i.e., third-party audits though tools like a business partner code of

conduct or a G&E register) or measure results, as well as for training purposes.

These tools can help to narrow the focus of compliance practitioners for maximum effectiveness. Without appropriate human evaluation in the right light however, even the smartest technology tool may be deemed useless.

Key Takeaways

Although two new pieces of legislation provide compliance practitioners with a compelling reason to revisit risk, along with internal reporting mechanisms, 'scare tactics' related to corporate accountability are unlikely to be viewed positively by management. Instead, use the shifting regulatory environment to demonstrate how the robust compliance protocols encouraged by the new guidance can be good for business, even when conditions normalize.

After all, the World Economic Forum has downgraded Germany from third to seventh place in its competitiveness index. Capital and regulatory requirements make it more difficult to start a business in Germany than in neighboring Denmark or the Netherlands. And while all political parties want to encourage business creation, business leaders should not rely on a "bureaucracy-free" regime or, the status quo in terms of regulatory oversight under the new *Bundestag*.

About the Author

Julia Arbery, a Partner with StoneTurn, has more than 15 years of experience in ethics and compliance. Specifically, she assists multinational corporations with the development and implementation of effective ethics and compliance programs across their global operations.