COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE RISK ANALYSIS

The article is an updated version of a presentation by Dr. Christian Rosinus at the Liechtensteiner Gespräche

Julian Zündorf-Girard

AUTHOR

Julian Zündorf-Girard is an attorney-at-law at Rosinus| Partner Rechtsanwälte PartG mbB. After earning his graduate degree in law from the University of Cologne (Germany) he completed his legal clerkship in Hanau (Germany). Mr. Zündorf-Girard is currently pursuing an executive master's degree in international criminal law at the University of Liechtenstein.

TABLE OF CONTENTS

I. INTRODUCTION

German Criminal law is built on the idea of personal criminal liability and only individuals can commit crimes. The idea of a special corporate criminal law has been discussed for years but was never established.[1] If such crimes are committed during a company's corporate actions, the company itself may face consequences. There are special rules for company fines[2] or confiscation orders against companies if their representatives commit offences on behalf of the company. Both may be issued independently of criminal proceedings against the individuals. A common predicate offence for such company fines or confiscation orders is the breach of supervisory duties pursuant to section 130 of the German Act for Administrative Offences (Ordnungswidrigkeitengesetz – OWiG). This offence requires that the owner of a company or certain other representatives or agents breach their duty to take necessary, appropriate and reasonable supervisory measures to prevent criminal and administrative offenses by employees.[3] When assessing company fines under the German administrative offences act, authorities and courts must take into account whether a company has installed an efficient compliance management system designed to prevent legal violations.[4] This results in a strong incentive for companies to install a compliance management system, even if they are not legally obliged to.[5]

II. RISK ANALYSIS

The basis of every compliance management system must be a compliance risk analysis as a company can only counteract risks that it knows about. Risks must be assessed specifically for each company because each company has its own risk profile. This results from the fact that the structure, products, and corporate culture of each company is different. Therefore, there is no "one size fits all"-solution when it comes to risk analysis. However, risk analysis generally follows the following basic three steps.

1. Identifying structural compliance risks in and for the company;
2. Assessing the compliance management system which is already in place;
3. Evaluation of risks, i.e., consequences and probability of occurrence.

A. Identification of risks

First of all, knowledge of the relevant legal obligations is central to the identification of risks. In addition, the company, its activities and the operating environment are decisive for the risks. For example, companies in the construction industry have different risks than companies in the defense industry, and global corporations have different risks than local medium-sized companies. The defense industry may face compliance challenges regarding proliferation, while a company in the construction industry

[1] See Sebastian Jungermann CEJ volume 5 (2019), p. 2-10.

[2] Sec. 30 German Act for Administrative Offences.

[3] Klaus Rogall, in Mitsch (Ed) *Karlsruher Kommentar zum Ordnungswidrigkeitengesetz* § 130, margin no. 34 ff.

[4] German Federal High Court of Justice, Judgment dated 9. May 2017, 1 StR 265/16, margin no. 118.

[5] Legal obligations may follow from Sec. 25a German Law on the Credit System (Kreditwesengesetz – KWG)

has a higher probability of challenges regarding occupational safety and illegal immigration. The location of the activity must also be taken into account. For example, operating in certain regions may have a higher risk of corruption according to the Corruption Perceptions Index[6].

B. Structural analysis

In addition to identifying the risks, the compliance structures already in place in the company must be examined. This is called structural analysis. In particular, a company should determine whether there are already guidelines, for example a code of conduct, or special guidelines against money laundering, corruption, or an antitrust guideline. Other structural features of a compliance management system are special staff trainings regarding compliance issues and detailed process descriptions. In training courses, employees are made aware of dangers for the company and of particular risks of criminal liability in connection with their activities in the company, and it is explained to them which behaviors can be advantageous in certain situations to mitigate risks or avoid them altogether. Other features of a compliance management system may include instructions for staff regarding the use of IT and passwords.

C. Analysis and evaluation of risks, i.e. consequences and probability of occurrence

The third step is a concrete analysis and evaluation of the risks. Here, the identified compliance risks must be examined with regard to their possible consequences for the company and the probability of their occurrence. These risks can then be compared with the compliance measures already in place to determine an overall risk profile. The analysis and evaluation of risks should be based in particular on operational risks and previous experience. In addition, it is relevant which persons and departments make decisions for the company and conclude contracts for the company. They should be analyzed with a special focus because they are especially prone to risks.

This serves as a basis for the further development and improvement of the compliance management system. Possible methods for this are the use of questionnaires to survey stakeholders, interviews, or site visits. There are also legal tech-tools which can be used to assist in such stakeholder surveys. Involving external consultants can be useful for this step, as they have a more objective view of the risks and are already experienced in creating questionnaires and conducting interviews. In particular, it seems favorable if interviews are conducted by attorneys, as they are legally bound to secrecy.[7] Based on practical experience, this also leads to more representative responses in some cases because staff members are oftentimes more open to discuss structural issues knowing that their identity will not be revealed.

When analyzing and prioritizing the identified risks, the financial impact, the probability of occurrence, and the timeframe in which a compliance violation may occur, play a role. For a final analysis, the results of the three steps must be compared in order to develop possible measures. The risks that the company is prepared to accept must also be taken into account. In any case, there is no such thing as no risk. A small risk always remains. The results can be presented in a report that color-codes the risks

[6] https://www.transparency.org/en/cpi/2021/.

[7] Sec. 203 para. 1 German Criminal Code.

(for example, using a traffic light system). Here, the color green stands for a low risk, yellow for a medium risk and red for a high risk.

III. CONTENTS

Special risk areas that are usually examined in many companies are, risks arising from corruption and antitrust law. In addition, depending on the company's operating activities, there are other risk areas, for example labor law risks.[8] One point of focus should always be the corporate culture with regard to compliance. In particular, the "*tone from the top*" plays a decisive role. This means that the company's management sets an example of compliance, makes a clear commitment to compliance with the law and other non-legal frameworks, and incorporates this into the company's day-to-day operations. Secondly, the "*zero tolerance principle*" plays a key role. According to this principle, violations of legal and compliance regulations are punished as a matter of principle. A third key aspect of the corporate culture is the error culture. This includes, for example, the question of whether employees can report errors without fear of consequences[9] or if there are even incentives to make suggestions for improvement.

IV. DEFINITION AND IMPLEMENTATION OF MEASURES TO AVERT RISKS

Companies can take measures to mitigate the identified risks. Of course, an existing compliance management system must be taken into consideration. Supplementary measures can be, for example, a code of conduct or further special guidelines, training of employees in particular about the identified risks, or further financial and personnel resources for the compliance officer or compliance department. The measures should be prioritized to mitigate the greatest risks first. In doing this, the company has discretion as to which priorities it sets. To check whether the measures are effective, it is advisable to carry out compliance risk analyses at regular intervals (e.g. annually) and in the event of significant changes in the company or the legal situation. By doing so, the improvement of the compliance management system also always reduces the required effort.

V. OUTLOOK

Risk analyses are the basis for any compliance management system, as they are a necessary means of identifying compliance risks and implementing the necessary measures. In some specific areas, risk analysis has therefore already become a legal obligation. In German law, for example, the obligation to conduct a special risk analysis for supply chain compliance has now been introduced.[10] This involves analyzing and assessing certain risks posed by suppliers to the environment and human rights, and taking countermeasures where necessary. There is a possibility that further, special obligations for risk analyses will be added in the future. In doing so, however, companies can draw on previous experience.

[8] In Germany especially legally limited working hours, occupational safety or workplace discrimination and mobbing.

[9] In many

[10] Sec. 5 German Code on Corporate Due Diligence to Prevent Human Rights Violations in Supply Chains.