Overview and practical advice on the German Whistleblower Protection Act

THE FINAL ACT (FOR NOW): THE WHISTLEBLOWER PROTECTION ACT IS NOW ALSO MANDATORY FOR COMPANIES WITH AT LEAST 50 EMPLOYEES

Overview

The German Whistleblower Protection Act aims to improve the early detection of misconduct in day-to-day business operations, and thus improve the affected companies' ability to respond to such misconduct, in line with long-standing international compliance management practice.
In addition, the legislation also provides comprehensive protection for whistleblowers. In summary, the following requirements apply:

- Companies of any legal form, ownership structure or industry sector affiliation with 50 or more employees are obliged to set up a whistleblowing system in the form of an internal reporting office. Companies that employ between 50 and 249 employees have until 17 December 2023 to implement this requriement.
- A company's internal reporting office can either be staffed with qualified employees of the company who act independently in this role. Alternatively, companies may choose to engage an external service provider.
- In principle, the company can decide whether information is to be received verbally or in text form. Ideally, both options should be made available in the interest of better documentability and, ultimately, legal certainty. A face-to-face meeting must also be made possible at the whistleblower's request.
- Companies do *not* have to make it possible for whistleblowers to submit information anonymously. However, the internal reporting office should follow up on any anonymous information it receives.

- Confidentiality with regard to the identity of the whistleblower as well as other parties mentioned by name in a report and compliance with data protection requirements must be ensured when reports are made to the internal reporting office and during processing of the report by the reporting office.
- If a whistleblower submits a report to the internal reporting office, the internal reporting office must confirm to the whistleblower that it has received the report within seven days.
- The reporting office must inform the whistleblower within three months about what measures have been taken ("**follow-up measures**"), such as the initiation of internal compliance investigations or the forwarding of the report to a competent authority, such as a law enforcement agency.
- Another equivalent option for submitting reports has been set up in the form of an external reporting office (currently) at the Federal Office of Justice (BfJ). Additional reporting offices have been set up at the Federal Cartel Office (BKartA), the Federal Financial Supervisory Authority (BaFin) and various federal states. Whistleblowers are free to decide whether they want to submit a report to their company's internal reporting office or use an external reporting office. There is no hierarchy between the internal and external reporting offices that the whistleblower must observe. However, companies are free to indicate a preference for whistleblowers to use their internal reporting office.
- Any adverse treatment of a whistleblower in response to their report is prohibited. To protect the whistleblower from retaliation, the legislation specifies a far-reaching reversal of the burden of proof: If a whistleblower is penalised in connection with their professional work, it is presumed (with the possibility for the company to refute this) that this constitutes retaliation for submitting the report and is thus unlawful. In addition, claims for damages by the whistleblower may come into play.
- Certain breaches of the provisions of the Whistleblower Protection Act by companies also constitute administrative offences. For example, failure to establish a reporting office, a breach of confidentiality or retaliating against a whistleblower are administrative offences. Depending on the type and severity of the breach, these offences can be punished with fines of up to EUR 50,000, and under certain circumstances up to EUR 500,000.

I. Background

The Whistleblower Protection Act transposes Directive (EU) 2019/1937 (hereinafter "**EU Directive**") into German law. The aim of the Whistleblower Protection Act and the EU Directive on which it is based is to improve the protection of persons who provide information about misconduct in companies. For instance, the law requires companies above a certain size to establish reporting offices for whistleblowers to turn to, while also prohibiting retaliation against persons who make legitimate use of these reporting channels.

II. Scope of application

1. Obligated companies

Companies fall under the scope of application of the Whistleblower Protection Act if they generally employ at least 50 people.

In addition, certain companies are subject to the Whistleblower Protection Act regardless of how many employees they have, such as capital investment companies and insurance companies pursuant to Section 12 (3) of the German Whistleblower Protection Act.

The number of employees is not determined on a specific reference date, but is based on the usual number of employees. Part-time employees are counted as full-time employees. In groups of companies, the employees are not added together (e.g. for the respective parent company); instead, each company must be examined separately to determine whether it meets the crucial threshold of 50 employees.

The number of employees also determines the deadline by which the company needs to have implemented the provisions of the Whistleblower Protection Act at the latest. Companies with 250 or more employees were obliged to comply immediately after the law came into force on 2 July 2023. Companies with between 50 and 249 employees have an extended implementation deadline to comply with the requirements until 17 December 2023.

2. Subject of reports

A crucial aspect with regard to the procedure following the receipt of a report and the protection of the whistleblower is the question of what types of irregularities should or can be reported in the first place. This is because not all breaches of law or other irregularities within companies fall within the scope of the Whistleblower Protection Act. Due to its limited legislative reach, the EU Directive only refers to breaches of European law. The national legislators of the EU member states were thus given leeway to specify which violations should now fall within the scope of application of the respective national law.

Section 2 of the German Whistleblower Protection Act contains an exhaustive list of the breaches covered by the German legal provisions. The scope of protection includes, in particular, breaches of criminal law and breaches that are subject to administrative fines. However, breaches subject to administrative fines only fall within the scope of the Whistleblower Protection Act insofar as they serve to protect life, limb or health or the rights of employees or the representative bodies. This includes, for example, breaches of occupational health and safety provisions or of the German Minimum Wage Act.

In addition, all breaches of federal and state legislation adopted to implement specific European regulations listed in the Whistleblower Protection Act are included, as well as breaches of directly applicable EU legal acts in a variety of different, specifically named areas.

Breaches that are not explicitly listed in Section 2 of the Whistleblower Protection Act do not fall within the scope of the law. This has an impact in particular on legal protection for whistleblowers. This is because the protection provided by the Whistleblower Protection Act is only effective if the reported breaches fall within the scope of the law or if the whistleblower had reason to believe that they did.

Liability risks for the company may arise if it cannot be determined with certainty whether reported breaches fall within the scope of application. It should therefore be ensured, even in cases of doubt, that the protective provisions in favour of the whistleblower are complied with.

Practice note:

In our view, several approaches could be considered. On the one hand, the company could explicitly limit the scope of application to the areas required by (German) law and only make the reporting office available for reports relating to such breaches. However, from a compliance perspective, reports received by the reporting office should not be ignored by the company simply because they do not fall within the scope of the whistleblower system. This is because the company's management has a duty – entirely independently of the Whistleblower Protection Act – to investigate and remedy any irregularities within the company ("Legalitätspflicht" – duty to adhere to applicable laws). However, the prescribed procedures under the Whistleblower Protection Act would then not be relevant in this respect and the protective effect in favour of the whistleblower would not apply. On the other hand, limiting the scope of the internal reporting office in this way would deprive the company of a broadly accepted point of contact for reporting other internal irregularities

and a means of systematically investigating such irregularities.

Alternatively, the company could therefore deliberately define the scope of application quite broadly, for example, by also including breaches of company policies. However, it will then have to be clarified whether the protective effect of the law (especially with regard to confidentiality and the prohibition of retaliation) is also extended to the reporting of such breaches. In this respect, this could lead to a certain potential for abuse, i.e., employees could report incidents that are of blatantly minor significance in order to be able to claim whistleblower protection. If, on the other hand, all breaches can be reported to the same reporting office, but the legal protection only applies within the scope of the Whistleblower Protection Act, this limited protective effect must be indicated in a transparent and comprehensible manner. However, it is not yet foreseeable how differentiating between reports in this way should best be handled in practice and how the courts in particular will view such a differentiation. In our opinion, it is therefore advisable to comprehensively observe the provisions of the Whistleblower Protection Act with regard to the procedure to be followed when making the reporting office available for reports on irregularities that go beyond the legal scope of application.

3. Persons entitled to report

According to the Whistleblower Protection Act, persons are entitled to report if they have obtained information about breaches in connection with their professional activities or prior (in the run-up) to such activities (Section 1 (1) Whistleblower Protection Act).

In contrast, the scope of application does not cover persons who have not gained knowledge of breaches "in connection with their professional activity" but, for example, in a private context. Further information on which persons must or should be allowed to submit reports to an internal reporting office can be found in the section below on internal reporting offices.

III. Reporting offices and reporting options

The German Whistleblower Protection Act provides for internal reporting offices of companies and external reporting offices established by the state.

Currently, there is an external state reporting office at the Federal Office of Justice. Additional reporting offices are set up at the Federal Cartel Office (BKartA), the Federal Financial Supervisory Authority (BaFin) and various federal states. Companies' internal reporting offices must provide clear and easily accessible information on these external reporting offices (Section 13 (2) Whistleblower Protection Act).

The establishment of an internal reporting office is the central duty established by the Whistleblower Protection Act (Section 12 Whistleblower Protection Act).

1. Organisation and staffing

An internal reporting office can be established by entrusting a person or a team employed by the respective company or an external third party with the tasks of an internal reporting office (Section 14 (1) Whistleblower Protection Act).

In both cases, it must be ensured that the appointed persons have the necessary independence and expertise (Section 15 Whistleblower Protection Act).

The persons entrusted with running an internal reporting office must be independent in the exercise of their duties. They must not be bound by instructions from the company with regard to their activities in connection with the reporting office and the handling of information. For example, they must not be instructed to conduct reporting procedures in a certain way. There must also be no conflicts of interest. The necessary expertise, especially legal and forensic knowledge, should be ensured through regular training when deploying company employees, especially with regard to the complex legal situation concerning the scope of application of the Whistleblower Protection Act as well as with regard to the correct handling of reports.

Practice note:
In our experience, companies often commission external service providers or ombudspersons, or the reporting office is set up internally within the role of the compliance officer or the legal department. The fact that employees of the company also perform other tasks in addition to their work for the internal reporting office is generally not a problem, provided that the necessary independence can still be ensured. It is advisable to record and document the independence from instructions and measures to prevent conflicts of interest as well as measures to ensure the employee has the necessary expertise when appointing the employee and, if required, at regular intervals.

2. Right to report to the internal reporting office

The internal reporting office is primarily aimed at receiving reports from employees (Section 12 (1) Whistleblower Protection Act). The term "employee" is defined in Section 3 (8) of the Whistleblower Protection Act, and includes – e.g. for private employers – in particular employees and trainees. In addition, the internal reporting office must also be available to temporary workers (Section 16 Whistleblower Protection Act). Companies may voluntarily make their internal reporting system available to third parties, but are not obliged to do so.

Practice note:
In many cases, it is advisable to deliberately make the internal reporting office available to persons other than the company's own employees, i.e., external third parties. This generally includes contractual business partners such as suppliers and subcontractors. Depending on the size of the company, companies with more than 3,000 domestic employees (as of 1 January 2024: with more than 1,000 domestic employees) are also obliged to set up a complaints procedure to report violations of human rights and environmental protection due diligence obligations, including by third parties, in accordance with Section 8 of the Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz – LkSG). In practice, this often leads to existing reporting offices being made available to a broader group of individuals. In general, it should be of great advantage if companies can find out about irregularities and violations as quickly and directly as possible by broadening the scope of their reporting channels – regardless of whether the reports originate from its own employees or third parties such as suppliers or contractual partners.

3. Reporting options

Pursuant to Section 16 (3) of the Whistleblower Protection Act, it must be possible to submit reports to the internal reporting office orally or in writing. The obliged company can therefore decide which of the two options it will make available. For reasons of legal compliance, however, we believe it is advisable to offer both options.

In addition, a face-to-face meeting with a responsible person at the reporting office must be made possible within a reasonable period of time at the whistleblower's request (Section 16 (3) sentence 3 Whistleblower Protection Act). In the case of an international reporting office, this task can also be delegated to a person on site. With the consent of the whistleblower, a meeting via video and audio is also sufficient (Section 16 (3) sentence 4 Whistleblower Protection Act).

It must be possible to submit reports at least in the predominant language of the employment or work environment.

The necessary confidentiality must be ensured for each reporting option made available (Section 8 Whistleblower Protection Act). The identity of the person providing the information as well as the identity of other persons named in the report must be protected from third parties.

Finally, reporting offices must provide clear and easily accessible information on external reporting offices (Section 13 (2) Whistleblower Protection Act).

Practice note:
Practice note: Oral reports must be made possible by telephone or another form of voice transmission, e.g., a whistleblower hotline or an answering machine system.

Reports in written form can also in principle be submitted via e-mail. In practice, we believe it is preferable to offer an IT-based whistleblowing system on the internet or intranet. The advantage of an IT tool over a simple e-mail address as a reporting channel is that the tool can guide the whistleblower through a series of questions. Firstly, a (pre-set) series of questions might be more user-friendly for the whistleblower when submitting their report, whereas when submitting a report via e-mail, it is up to the whistleblower to decide for themselves which information may be relevant for an investigation. Furthermore, the internal reporting office benefits if the key points and information for processing the report have already been requested when the report is submitted. In this way, the necessary information can be presented more clearly and/or requests for certain information can be better coordinated, while at the same time ensuring confidentiality in a comprehensive manner. In any case, confidentiality must be ensured for each reporting option that is made available. Furthermore, it must be ensured that employees are provided with relevant information about the external reporting procedure and external reporting offices.

4. Group-wide central reporting office

The question of whether a single central reporting office can be set up within a group of companies to receive and process reports from all group companies or whether each group company that falls within the scope of the Whistleblower Protection Act or a corresponding foreign regulation must set up its own reporting office has not yet been conclusively clarified. In a legally non-binding opinion, the European Commission considers a group-wide reporting office to be incompatible with the EU Directive.[1] However, Art. 8 (6) sentence 1 of the EU Directive expressly permits companies with 50 to 249 employees to share resources not only in processing and investigating reports, but also in receiving them. It is therefore permissible for companies of this size to operate a joint reporting office.

The German Whistleblower Protection Act does not make any explicit statement on the admissibility of a group reporting office. However, in the explanatory memorandum to the law, the German legislator considers such a central reporting office at a group company to be permissible, irrespective of how many employees the company has.[2] In this respect, the current view is that a centralised, group-wide reporting office can be established without the threat of fines (in Germany). Whether a group reporting office will be permissible on a permanent basis depends on whether and how the ECJ will rule on this legal question.

Practice note:

In our view, there are good arguments in favour of setting up a central reporting office within a group of companies. Functions can be bundled there, and structures for the processing of reports can be made more efficient. Concentrating the processing of reports in a central reporting office also means that the members of the reporting office can gain more extensive experience with incoming reports more rapidly and thus increase their practical and professional expertise. Additional obligations to set up reporting offices under other legal provisions such as the LkSG or the General Equal Treatment Act also make a central bundling of functions practical.

On the other hand, a local reporting office often has a better and faster understanding of whether a report is plausible and whether a report falls under the material scope of application of the respective national law. Furthermore, if the report concerns a specific (subsidiary) company, it is usually necessary to examine the content of such a report at the level of the (subsidiary) company. In addition, the (subsidiary) company must be involved in the processing of the report about an irregularity on the level of the same (subsidiary) company anyway due to its duty to adhere to applicable laws, meaning that it is hardly ever possible to process reports entirely centrally at the level of the parent company alone. If the subsidiaries lack the resources or expertise for follow-up measures and extensive internal investigations, these resources can be provided by the

[1] JUST/CO/MM/rp/ (2021)3939215 dated 2.6.2021 and JUST/CO/MM/rp/ (2021)4667786 dated 29.6.2021.

[2] BT-Drs. 20/3442 p. 79.

parent company in accordance with Article 8 (6) sentence 1 of the EU Directive or third parties can be entrusted with carrying out such follow-up measures on the basis of Article 8 (5) of the EU Directive.

It may thus also be advisable to establish different reporting offices at the parent company and at the subsidiary and/or set up parallel reporting channels, provided that the structures are aligned and the processing of information is coordinated and carried out with a consistent level of expertise.

5. Anonymity

There is no obligation on the part of the company to allow anonymous reports to be made via the internal reporting office (Section 16 (1) sentence 5 Whistleblower Protection Act). However, if the reporting office receives anonymous reports, these "should" also be processed (Section 16, (1), sentence 4 Whistleblower Protection Act).

Anonymous whistleblowers are covered by the protective provisions of the Whistleblower Protection Act if their initially concealed identity later becomes known.

Practice note:
It may be desirable for companies to explicitly allow anonymous reporting, e.g., for employees to make first contact with the internal reporting office. It must then be ensured that the reporting options do in fact allow for anonymous reporting.

The ability to submit anonymous reports often lowers the inhibition threshold for whistleblowing significantly. Whistleblowers very often find themselves in a personal dilemma and therefore shy away from making a report which could potentially have a far-reaching and critical impact on the company due to deep-rooted feelings of doubt and uncertainty. Voluntarily allowing anonymous reporting can therefore make a company's internal reporting channels more attractive.

If a company decides to make the internal reporting channel available for anonymous reports as well, the question arises as to what type of reporting channel is best suited for this purpose. The use of a telephone hotline has the disadvantage that the whistleblower cannot transmit documents and the reporting office cannot get in contact with them if it has any queries. It is not clear whether it is possible for a whistleblower to submit a report anonymously via e-mail. In any case, if the whistleblower sends documents by e-mail, the metadata of the documents may allow conclusions to be drawn about the identity of the person sending the documents. Using an IT tool for submitting a report may also be preferable in this respect, since anonymity can be technically ensured and the whistleblower and the reporting office can communicate with each other via technical means while maintaining anonymity, provided the whistleblower is willing to do so. From a technical standpoint, it is possible to issue a confirmation of receipt and feedback to the whistleblower while maintaining anonymity.

6. Compliance with data protection regulations

When setting up and operating the internal reporting office, data protection regulations must be complied with and the necessary measures need to be taken. For example, when selecting the reporting channel, suitable technical and organisational measures must be taken in accordance with Art. 32 GDPR. When involving external third parties in the operation of the internal reporting office or when setting up a group reporting office, it should be checked whether additional agreements regarding data protection need to be concluded.

In addition, data protection documentation (such as data protection notices for whistleblowers when submitting a report, additions to the record of processing activities along with a deletion concept, a data protection impact assessment within the meaning of Art. 35 GDPR or declarations of confidentiality by the persons employed in the reporting office) may need to be adapted or created.

7. Involvement of the works council

If there is a works council, co-determination rights may have to be observed when setting up and operating the

internal reporting office. In this context, the co-determination right under Section 87 (1) sentence 1 of the Works Constitution Act (BetrVG) in particular comes into consideration, insofar as the organisational conduct in the company is affected, as well as a co-determination right under Section 87 (1) no. 6 BetrVG with regard to the introduction and use of technical equipment suitable for monitoring performance or conduct. Whether and to what extent co-determination rights exist for certain aspects of the establishment and operation of a reporting office may also depend on the specific design of the reporting system.

Practice note:

Involving the works council in an exchange of information and opinions with regard to the requirements and the specific situation in the company and the most suitable means of implementation early on can be helpful and expedient during the necessary preliminary considerations when setting up a whistleblowing system. In our view, works councils may also be involved in order to ensure that the whistleblowing system is as widely accepted as possible among the workforce. With this in mind, it is important to clarify any potential statutory co-determination rights in advance. That being said, in our view, the works council should be involved in the establishment and design of the whistleblowing system at an early stage, regardless of any legal obligation to do so.

8. Relationship between internal and external reporting offices

Whistleblowers have the right to choose between internal and external reporting offices. However, they should give priority to internal reporting offices, provided that effective internal action can be taken against the breach and they are not concerned about retaliation.
Companies should provide incentives for whistleblowers to contact the respective internal reporting office first before turning to an external reporting office. Clear and easily accessible information on the use of the internal reporting procedure should be provided. However, this must not restrict or impede staff from making an external report (Section 7 (3) Whistleblower Protection Act) and information on external reporting procedures must be provided (Section 13 (2) Whistleblower Protection Act).

Practice note:

A company's goal should be to make the company's internal reporting office as attractive and trustworthy as possible, to provide easy access and to encourage employees to use the internal reporting office. The granting of financial rewards is also being discussed as a possible incentive to encourage employees to use the internal reporting office (for example, such financial incentive systems are becoming increasingly common in the USA). Although the Whistleblower Protection Act does not rule out such incentives per se, it is doubtful whether this is a sensible course of action. In any case, such an incentive system is unlikely to be conducive to a positive working environment.

IV. Obligations after receiving a report

The procedure to be followed and the tasks of the internal reporting office after receiving a report are specified in Section 17 and Section 11 of the Whistleblower Protection Act.

1. Acknowledgement of receipt

First of all, the reporting office must acknowledge receipt of a report within seven days (Section 17 (1) no. 1 Whistleblower Protection Act).

2. Review

The internal reporting office will then examine whether the reported violation or irregularity falls within the material scope of application of the Whistleblower Protection Act. If this is the case, the internal reporting office will evaluate the validity of the report received and, if necessary and feasible, request further information from the whistleblower. Once the internal reporting office has gained a sufficient factual basis, it will conclude its examination of the report (Section 17 (1) nos. 2 to 5 Whistleblower Protection Act).

3. Follow-up measures

The reporting office must then take appropriate follow-up measures (Section 17 (1) no. 6 and Section 18 Whistleblower Protection Act). Pursuant to Section 18 of the Whistleblower Protection Act, follow-up measures may include the initiation of internal investigations, referring the whistleblower to other competent bodies, or handing over the proceedings to a competent authority (e.g., law enforcement authority).

4. Feedback to the whistleblower

Finally, the reporting office must provide feedback to the whistleblower (Section 17 (2) sentence 1 Whistleblower Protection Act) on any measures that are planned or have already been taken as well as the reasons for this action within three months of the acknowledgement of receipt.

Feedback does not have to be provided if this would affect the investigation or impair the rights of individuals concerned.

5. Documentation of incoming reports

Pursuant to Section 11 (1) of the Whistleblower Protection Act, the internal reporting office will document incoming reports in a permanently retrievable manner in compliance with the confidentiality requirement. The documentation must be deleted three years after the conclusion of the procedure. It may be kept for longer if this is necessary and proportionate under the Whistleblower Protection Act or other legal provisions (Section 11 (5) Whistleblower Protection Act).

The documentation is also kept to preserve evidence for potential legal proceedings. This serves to protect both the whistleblower and the company, for example, if the whistleblower seeks legal defence against “retaliation” from the company and the company is obliged to prove that such actions are not related to the whistleblower’s report.

V. Protection of the whistleblower

1. Confidentiality requirement

Internal reporting offices must treat the identity of the whistleblower as confidential, at least if the report falls within the material scope of application of the Whistleblower Protection Act or the whistleblower could reasonably assume that this would be the case.

The obligation of confidentiality also includes the identity of the persons accused of misconduct and other persons named in the report, such as colleagues (Section 8 (1) sentence 1 nos. 2 and 3 Whistleblower Protection Act). Information from which the identity of these persons could be deduced is also covered by confidentiality.

According to Section 8 (1) sentence 2 of the Whistleblower Protection Act, the identity of these persons may only be made known to the members of the internal reporting office or to the persons responsible for taking follow-up measures, as well as to the persons supporting them in the performance of these tasks (such as office or IT staff).

Whistleblowers cannot invoke the confidentiality requirement if they intentionally or through gross negligence submit incorrect reports. The further exceptions to the confidentiality requirement specified in Section 9 of the Whistleblower Protection Act mainly concern cases in which disclosure is requested by a public authority or a court, for example in connection with criminal

proceedings. Other than this, the internal reporting office may only disclose the identity of the whistleblower if the disclosure is necessary for follow-up measures and the whistleblower has previously consented to the disclosure. The identity of other persons may be disclosed if the person consents to the disclosure or if the disclosure is necessary in the context of internal investigations at the company or for taking follow-up measures.

2. Protection from retaliation

The Whistleblower Protection Act protects whistleblowers from retaliation in connection with submitting a report. The term "retaliation" includes any action or omission in a professional context that may have a negative impact on the whistleblower and that is a reaction to the whistleblower submitting a report (Section 3 (6) Whistleblower Protection Act). Such disadvantages can include, for example, suspensions, dismissals or wage cuts. It is not only actual retaliation against whistleblowers that is prohibited, but also the threat of retaliation or attempted retaliation (Section 36 (1) Whistleblower Protection Act).

The question of whether adverse treatment is a reaction to a report (and thus retaliation) is subject to a reversal of the burden of proof under the law: If the whistleblower claims that the specific treatment is a reaction to their report, this is presumed to be true (Section 36 (2) Whistleblower Protection Act). The company must then demonstrate that there was no link between the treatment of the whistleblower and the report or that the treatment of the whistleblower was based on sufficiently justified reasons. The law does not set a fixed time limit for this presumption rule; however, the presumption is likely to weaken with the passage of time.

If the company violates this prohibition of retaliation, the whistleblower (or other persons pursuant to Section 34 of the Whistleblower Protection Act) may have a claim for compensation of resulting damages (Section 37 Whistleblower Protection Act).

VI. Consequences of breaches of the company's obligations under the Whistleblower Protection Act

Section 40 of the Whistleblower Protection Act contains a list of administrative offences that may occur through a breach of the obligations resulting from the Whistleblower Protection Act.

If an internal reporting office is not set up or operated although the company is obliged to do so, this constitutes an administrative offence that can be punished with a fine of up to EUR 20,000. Other breaches can result in fines of up to EUR 50,000, such as

- obstructing or attempting to obstruct a report or communication in connection with a report,
- retaliation or attempted retaliation, or
- a deliberate or grossly negligent failure to maintain confidentiality.

Under certain circumstances, the maximum fine may also rise to EUR 500,000.

Section 40 of the Whistleblower Protection Act is designed as an "everyman's" offence, meaning that it can in principle be committed by any natural person. Section 130 of the German Administrative Offences Act (OWiG) is also applicable in relation to Section 40 of the Whistleblower Protection Act, which penalises the wilful or negligent failure to exercise proper supervision by the owner of the business or company. The company itself may also face sanctions pursuant to Sections 130 and 30 OWiG, even if the direct violation of Section 40 of the Whistleblower Protection Act was not committed by a manager within the meaning of -Section 30 (1) OWiG. If a corporate fine can be imposed in accordance with Section 30 OWiG, Section 40 (6) sentence 2 of the Whistleblower Protection Act in conjunction with Section 30 (2) sentence 3 OWiG specifies a corporate fine. Section 30 (2) sentence 3 OWiG provides for a tenfold increase in the maximum fine. It should also be mentioned that fines of more than EUR 200 against a legal entity or its managers must be entered in the central trade register; in individual cases, this

can put companies at a disadvantage when bidding for public contracts.

VII. Recommendations

When implementing a whistleblower system, companies must first make some decisions regarding how to structure the system:

- Should the running of the internal reporting office be entrusted to employees of the company or to an external service provider?
- Where should the internal reporting office be located? Should there be a central group-wide reporting office or (if necessary additional) reporting offices in all/certain group companies?
- Which reporting options should be provided? Which (technical) solutions are available?
- What should the scope of application be? Should the scope of application also be extended to cover, for example, breaches of company policies? What does this mean for the level of protection of the whistleblower?
- Should anonymous reports be possible?
- Should it be possible for external third parties to submit reports?
- What structures and lines of communication should be in place within the company or the group for passing on information, examining reports and implementing follow-up measures?
- How is documentation to be carried out?

Furthermore, in particular the following documents may need to be prepared:

- If not already in place, a code of conduct should be developed and implemented. As a conscious description of the conduct expected of all employees, including all members of company management and executives, external third parties such as contractual business partners and customers, such codes of conduct can provide a material basis of reference for reports or information. Without a code of conduct, in the vast majority of cases, in particular for internationally operating companies, it is impossible to harmonise differently implemented European whistleblower protection laws for day-to-day operations. Considering the overarching objective of offering the lowest possible threshold to a large number of potential whistleblowers, it is simply not reasonable to also expect whistleblowers to decide which legal classification their report falls under. Without any prior legal knowledge, few employees going about their day-to-day work would be able to decide without assistance whether a report concerns a violation of EU law or national law or if regulations subject to penalties or merely a regulatory fine have been violated. Many years of international compliance management practice have shown that clearly communicated reference to a risk-based code of conduct leads to reliability in application and legal certainty.
- The whistleblowing system should be described as simply and comprehensibly as possible in a whistleblowing policy.
- An internal process description should be drawn up that defines the specific procedure to be followed by the internal reporting office after receiving a report. This should include the deadlines for acknowledging receipt and providing feedback to the whistleblower, specifications for documentation and deletion deadlines, a clear definition of responsibilities, and regulations for avoiding conflicts of interest.

- The delegation of the tasks of an internal reporting office to certain persons should be explicitly documented or contractually agreed upon. The corresponding rights and duties and responsibilities should be specified.
- In addition, some data protection documents may need to be adapted or to be supplemented, for example data protection notices within the meaning of Art. 13 GDPR for whistleblowers in connection with the submission of a report.
- The technical functionality and accessibility of the should be tested regularly by the company itself. These tests must be documented accordingly.
- Finally, the obliged company should communicate regularly and verifiably about the establishment and operation of the internal.

Nicole Deparade
Lawyer
Certified specialist for employment law
nicole.deparade@gsk.de

Dr Philipp Kuhn
Lawyer
Certified specialist for employment law
philipp.kuhn@gsk.de

Eric Mayer
Lawyer
Compliance
eric.mayer@gsk.de

Tobias V. Abersfelder, LL.M. (Nottingham)
Lawyer
Compliance und Investigations
tobias.abersfelder@gsk.de

Dr Martin Hossenfelder
Lawyer
Data Protection Law
martin.hossenfelder@gsk.de

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason, we recommend you to request personal advice.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxembourg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
London branch
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Registered office: Munich
Munich Local Court
HRB 281930
Managing directors:
Dr Mark Butt, Andreas Dimmling

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM