Baker McKenzie.

Client Alert

December 2022

Germany: The new German Whistleblower Protection Act

What lies ahead for companies and what to do now

In brief

The German Bundestag passed the German Whistleblower Protection Act on 16 December 2022. After initially not being expected to be passed this year, the bill did make it onto the agenda of the last session day of the year at short notice and was passed in a version amended by the Legal Affairs Committee (Rechtsausschuss) with the coalition's majority. The next step is for the Bundesrat to approve the bill. However, this is not expected until the first plenary session in February 2023 at the earliest.

In this issue

Key points of the law

Latest changes in the legislative process

Which companies have to implement a reporting system?

Who can be a whistleblower and who is protected?

What kind of reports are protected?

No priority for internal reporting channels

Core element: protection for whistleblowers — prohibition against reprisals, damages and fines

Dealing with anonymous reports

What applies to groups of companies with a central reporting channel?

What is in store for companies?

What should companies do now?

Key points of the law

- Companies with at least 250 employees are obliged to set up an internal reporting system when the law comes into force. For companies with 50 to 249 employees, this obligation will apply from 17 December 2023.
- Whistleblowers shall be comprehensively protected, in particular against reprisals. Any discrimination against a whistleblower in connection with a report is prohibited. The burden of proof lies with the companies.
- Whistleblowers are free to choose whether to report internally or externally. Public disclosures are only permitted in exceptional cases.
- Corporate groups can implement an internal reporting office at the group level.
- Companies must now also provide reporting channels for anonymous reports and process anonymous incoming reports - but here there is a longer implementation deadline of 2025, regardless of the size of the companies.
- The law enters into force three months after promulgation.

Latest changes in the legislative process

On 27 July 2022, the Federal Cabinet adopted a government draft of the Whistleblower Protection Act. The government draft was then discussed in the Bundestag in September and in a public hearing of the Legal Affairs Committee in October. Following a number of — in some cases very far-reaching — recommendations for amendments by the Legal Affairs Committee, the bill as amended by the Legal Affairs Committee was finally passed in the Bundestag on 16 December 2022.

Which companies have to implement a reporting system?

The obligation to introduce a whistleblowing system applies to companies with **at least 50 employees** (Section 12 (2) HinSchG). Irrespective of the number of employees, companies in certain sectors, such as financial service providers, are already obliged to set up whistleblowing channels under existing law.

Who can be a whistleblower and who is protected?

The personal scope of application of the HinSchG-E includes all persons who have obtained information about violations in connection with their professional activities (Section 1 (1) HinSchG). Primarily covered are employees of the company. In addition, companies can decide whether their reporting channels should also be open to third parties, such as contractors or suppliers (Section 16 (1) HinSchG). The HinSchG also protects the confidentiality needs of the persons who are themselves the subject of a report or affected by it (Sec. 1 (2) HinSchG). This applies to internal as well as external reports and to public disclosures.

What kind of reports are protected?

The HinSchG is intended to cover reports of "significant violations". This includes violations that are punishable by law (criminal offences) as well as violations that are punishable by a fine (administrative offences), the latter, however, only insofar as the violated regulation serves to protect life, limb, health or the rights of employees or their representatives such as works council members (Sec. 2 (1) HinSchG). Violations of the General Equal Treatment Act (AGG) are initially not included due to the lack of a fine. However, on the recommendation of the Legal Affairs Committee, the Bundestag has called on the Federal Government to examine whether whistleblowers are sufficiently protected when reporting violations of the General Equal Treatment Act (AGG) or comparable violations, so there could still be a tightening of the law relevant for companies in the future.

In addition to these general rules, the draft lists further violations that fall within the material scope of application, such as violations of rules on money-laundering prevention, product safety and conformity, environmental protection, data protection, etc. Public procurement and financial services are also relevant areas of law. Also included in the scope of protection are violations of various European laws. The scope of application covers both European and German antitrust law.

Excluded from the scope of protection are violations of internal company policies and guidelines (provided that there is no simultaneous violation of criminal laws, etc.) as well as unethical conduct. The extent to which companies can provide the reporting channels for such violations must be examined in detail, particularly from a data protection perspective.

Furthermore, the scope of protection only applies insofar as it concerns misconduct in connection with professional activity. Reports relating to misconduct in the private sphere are not protected.

No priority for internal reporting channels

Whistleblowers have the choice of reporting the information either to an internal reporting channel of the company or to an external reporting channel (Section 7 HinSchG). The external reporting channel is to be established at the Federal Office of Justice, but BaFin and the Federal Cartel Office are also to act as external reporting channels. The German legislator does not give priority to internal reporting procedures.

According to Section 7 (3) of the HinSchG, employers are now to create incentives for employees to first use internal reporting channels. The government draft had previously remained silent in this regard. Now, Article 7 (2) and (3) of the HinSch-RL is explicitly anchored in the wording of the law. However, whether and to what extent employers create corresponding incentives are deliberately not specified. We will have to wait and see what incentives companies will introduce. The only thing that is clear is that this must not restrict access to external reporting channels, for example through internal regulations or agreements.

Only in exceptional cases is it possible to publicly disclose information about violations (Section 32 HinSchG).

Core element: protection for whistleblowers — prohibition against reprisals, damages and fines

The HinSchG serves to protect whistleblowers. The primary protection is provided by the prohibition against reprisals (Section 36(1) HinSchG). The term reprisal is broadly defined and ranges from dismissal to disciplinary measures, but also covers mobbing, discrimination or exclusion. The threat of reprisals as well as the attempt to carry out reprisals are already prohibited. If whistleblowers are pressured into concluding a termination agreement by means of a reprisal, for example, this agreement is null and void.

The draft law provides for a reversal of the burden of proof in favour of whistleblowers. It is thus presumed that it is a case of reprisal if whistleblowers are disadvantaged in their professional activities after making the report. The company must then prove that there were sufficiently justified reasons for the discrimination or that there is no connection to the report.

In the event of a violation of the prohibition of reprisals, companies are obliged to compensate whistleblowers for damages, whereby whistleblowers are entitled to appropriate monetary compensation for damages that are not pecuniary damages, irrespective of the prerequisites of Section 253 (2) of the German Civil Code or the existence of a serious violation of the general right of personality (Section 37 (1) HinSchG).

In addition, reprisals can lead to a fine of up to EUR 100,000 (Section 40 (2) no. 3, (6) HinSchG). However, on the recommendation of the Legal Affairs Committee, the Bundestag has called on the Federal Government to evaluate whether the provisions on fines provided for in the Whistleblower Protection Act sufficiently take into account the different economic performances of companies. In this respect, the law may be tightened in the future in a way that is relevant for companies.

Dealing with anonymous reports

One of the most fundamental changes incorporated during the legislative process is that companies are now required to also process anonymous incoming reports and to provide reporting channels for this purpose, which enable anonymous contact and communication with the internal reporting channel. For the anonymous reporting channel, the same formal requirements (e.g., confirmation of receipt within seven days) apply as for non-anonymous reports. With this, the legislator goes far beyond the HinSch-RL and the original government draft. Neither had provided for a corresponding obligation, leaving it up to the companies to decide whether they wanted to allow anonymous reporting. The obligation to also process anonymous incoming reports and to provide reporting channels for this purpose will lead to a considerable additional effort for companies. It is probably little consolation that the legislator has linked the obligations to a longer transitional period until 1 January 2025 (Section 42 (2) HinSchG) and has also made it clear in the context of the tightening that the comprehensive catalogue of obligations should only apply to anonymous reports received via the reporting channel provided for this purpose. If whistleblowers submit reports by other means, for example by means of an anonymous letter without the possibility of contact, some formal requirements do not apply (e.g., confirmation of receipt within seven days) (Section 16 (1) sentence 6 HinSchG). However, the legislator also makes it clear that the internal reporting channel must process anonymous incoming reports, regardless of the reporting channel chosen.

What applies to groups of companies with a central reporting channel?

In the course of the legislative process, there was much discussion as to whether reporting channels set up centrally, e.g., at the parent company of the group, were sufficient or whether there is a need for independent local reporting channels. This was preceded by statements by the EU Commission in favour of a local solution. The HinSchG, like the government draft before it, positions itself in favour of the "group solution" and permits centrally organised whistleblowing systems. However, the primary responsibility to remedy identified violations remains with the local company.

The Legal Affairs Committee expressly reiterated this position in its recommendation for a resolution, pointing out the associated advantages for both companies and whistleblowers. However, the Legal Affairs Committee's indication that easy access for whistleblowers must also be ensured in the case of group-wide solutions, which should explicitly include reporting in the working language predominant for whistleblowers in the respective company, is likely to be of interest to companies.

However, how the other member states will position themselves remains to be seen. In the worst case, there is a risk of a patchwork with different requirements.

What is in store for companies?

The protection of whistleblowers touches on several areas of law. This was also one of the reasons why the transposition of the Whistleblower Directive has been delayed. These difficulties not only affect the legislators, but will also pose challenges for companies. In addition to the requirements of the Whistleblower Directive and the local implementation laws, companies will have to carefully examine how they can ensure compliance with **data protection requirements**. In this respect, the HinSchG remains cautious and states, for example, in Section 10 sentence 1 only that the reporting channels are authorised to process personal data insofar as this is necessary to fulfil the tasks assigned to them (Sections 13 and 24 HinSchG). A new provision was added to Section 10 sentence 2 HinSchG, which regulates that the processing of special categories of personal data by reporting channels is permissible if this is necessary to fulfil its tasks. Questions of data protection law arise not only with regard to the legal basis for a mutual exchange of information in connection with reports and subsequent investigations, but also with regard to notifications to the data subjects. In addition, how companies position themselves with regard to possible claims for information by the affected parties (accused reporters or other parties involved) also plays a role. If the group headquarters — and thus the investigative unit — is located outside the EU, the international transfer of data raises questions. This requirement may also play a role in other scenarios/constellations. In addition, many other data protection aspects must be taken into account (e.g., data protection declarations, data protection contracts, deletion concept and performance of data protection impact assessments). How the data protection authorities will position themselves also remains to be seen.

The deletion period pursuant to Section 11 (5) HinSchG was extended from two years to three years. The deletion period was the subject of fierce criticism in the legislative process, with demands for a longer, shorter or also fundamentally more flexible deadline solution. On the recommendation of the Legal Affairs Committee, the legislature has now opted for a rigid time limit of three years, which is based on the regular limitation period of Section 195 BGB. The argument against a flexible, case-by-case approach was that this would have placed the responsibility for the time of deletion on the respective reporting channels and would have generated correspondingly more work. With regard to the risk of preserving evidence for later legal disputes, which is frequently cited by companies, the legislator now merely refers to the fact that this preservation of evidence must be carried out "in good time".

In addition, **collective labour law aspects** play an important role in Germany and other member states.

Due to the large number of new requirements under the Whistleblower Directive and the Whistleblower Protection Act, it makes sense for companies to incorporate these into an internal set of rules in addition to setting up the corresponding reporting channels in order to be able to document that the company complies with the requirements of the applicable whistleblower protection laws.

In the course of this, companies should check whether the requirements are complied with in the individual whistleblower channels. Practical difficulties may arise, in particular with regard to confidentiality and data protection.

What should companies do now?

Currently, only 11 of the 27 member states have implemented the Whistleblower Directive. After France passed the corresponding implementation law at the beginning of 2022, many international corporations looked toward Germany with a wait-and-see attitude. Now that the German Whistleblower Act is (finally) available, the time has come to initiate the necessary adjustments in the European corporate units.

It has proven to be a resource-efficient approach to first develop a common denominator based on a company's core markets that takes into account the legal requirements of the core markets. This transnational standard can then be adapted for the smaller markets, provided the scope of application is open.

Contact Us

Dr. Nicolai Behr
Partner
Munich
nicolai.behr
@bakermckenzie.com

Katja Häferer
Partner
Frankfurt / Munich
katja.haeferer
@bakermckenzie.com

Florian Tannen
Partner
Munich
florian.tannen
@bakermckenzie.com

Dr. Michaela Nebel
Partner
Frankfurt
michaela.nebel
@bakermckenzie.com

Christian Koops
Partner
Munich
christian.koops
@bakermckenzie.com

Dr. Robin Haas, LL.M.
Counsel
Munich
robin.haas
@bakermckenzie.com

Marleen Kerstin Ellinger, LL.M.
Associate
Munich
marleen.ellinger
@bakermckenzie.com