

Whistleblower Protection Act in force

Need for action by employers

By Dr. Hagen Köckeritz, LL.M. oec. int.



Existing whistleblowing systems may need to be adapted, in particular to meet the increased requirements for confidentiality and documentation.

The German Whistleblower Protection Act (HinSchG) came into force on 2 July 2023. With this new act, the German legislature is (belatedly) implementing the EU Whistleblowing Directive (Directive 2019/1937). For the first time, the HinSchG creates a binding legal framework to protect whistleblowers across sectors. For employers who have not yet introduced an internal whistleblowing system, there will in principle be an obligation to set up internal reporting channels from 17 December 2023; for employers with at least 250 employees, this obligation has already existed since the law came into force. Employers with fewer than 50 employees are excluded from the scope.

Objective of the HinSchG

The HinSchG provides rules for the implementation of whistleblowing systems across all sectors that previously existed only for certain parts of the economy (e.g., Section 25a (1) Sentence 6 No. 3 of the German Banking Act, Section 58 of the German Securities Trading Act, Section 23 (6) of the German Insurance Supervision Act, and Section 6 (5) of the Money Laundering Act). Protection primarily means prohibition of reprisals. The HinSchG defines binding standards that must be observed when setting up reporting channels, handling incoming reports and dealing with whistleblowers. However, it also regulates the



Dr. Hagen Köckeritz, LL.M. oec. int.

Mayer Brown LLP, Frankfurt/Main
Rechtsanwalt, Partner

hkoeckeritz@mayerbrown.com
www.mayerbrown.com

consequences for whistleblowers if they submit false reports through gross negligence or even intentionally. In this respect, denunciation is prevented from the outset. In terms of content, the HinSchG largely implements the EU Whistleblowing Directive 1:1. In some areas, however, it goes beyond the directive, while in others it falls short of the directive's requirements (and opportunities).

Scope

The personal and factual scope of application of the HinSchG is generally broad.

Whistleblowers are all individuals who have obtained information about violations in connection with their professional activities and reported them. In addition to active and former employees, this also includes job applicants, interns and temporary workers. In addition, self-employed persons who provide services or works are also covered. Members of the administrative, management or supervisory bodies of a company may also be covered, without this of course diminishing or even nullifying the obligations under company law to monitor and act.

“Whistleblowers are all individuals who have obtained information about violations in connection with their professional activities and reported them.”

In factual terms, the HinSchG goes beyond the EU Whistleblowing Directive and is not limited to reporting violations of EU law. As a result, whistleblowers enjoy protection against reprisals if they report the following types of violations, among others:

- Criminal acts;
- Violations that are punishable by an administrative fine if the violated norm serves to protect life, limb or health or to protect the rights of employees or their representative bodies – covered are, for example, regulations on occupational health and safety (including working time law) and minimum wage provisions, as well as regulations on obligations to provide information and clarification to employee representatives such as works councils;
- Other violations of selected federal and state legislation and directly applicable legal acts of the European Union and the European Atomic Energy Community (as described in more detail in Sec. 2 no. 3 et seq. HinSchG).

Reporting channels

The HinSchG distinguishes between external and internal channels.

An external reporting channel has been set up by the Federal Government at the Federal Office of Justice. It is responsible for external reports unless the responsibility of

an external reporting office of the federal states or other more closely designated offices (e.g., BaFin, Federal Cartel Office) is justified.

More relevant for companies, however, are the internal channels. These must be set up by companies with at least 50 employees. For companies with generally at least 250 employees, this obligation has already existed since the law came into force. Companies with 50 to 249 employees will not have to set up and operate internal reporting units until December 17, 2023. This does not affect the obligation of companies in certain sectors of the economy, which are required to set up reporting offices regardless of their number of employees.

The HinSchG allows companies to transfer the establishment and operation of reporting channels to third parties (including other group companies). Under the Act, several employers with generally 50 to 249 employees can also set up and operate a joint reporting channel. According to general understanding, the possibility of transferring the tasks related to the reporting channel extends to all tasks. It is not limited to receiving reports, but may also include taking follow-up action. However, the ultimate responsibility for taking action to stop violations remains with the company in all such cases.

Internal reporting channels must be available at least to the company's own employees and temporary workers. However, they can also be designed in such a way that they are also open to other individuals who, in the course of their professional activities, are in contact with the respective employer obliged to set up the internal reporting

channel, or in contact with the respective organizational unit. Internal reporting channels must allow reports to be made verbally or in text form. At the whistleblower's request, a personal discussion shall also be made possible within a reasonable period of time. Enabling the receipt of anonymous reports is expressly desired, but is not mandatory.

Any co-determination rights of the works council and data protection provisions must be observed when designing internal reporting channels.

Right to choose between internal and external reporting

Whistleblowers have the right to choose between internal and external reporting. The HinSchG merely recommends that whistleblowers should give preference to internal reporting if effective internal action can be taken against a violation and the whistleblower does not fear reprisals. Moreover, the law encourages companies to create incentives for giving priority to the internal reporting channel. This is also recommended in practice, as it allows problems to be resolved more efficiently and without delay.

Confidentiality

For all reports, it must be ensured that the identity of the whistleblower, as well as of the persons who are the subject of a report or are otherwise mentioned in a report, is pro-

tected. The identity of the persons mentioned may only be known to the persons responsible for receiving the report and taking follow-up action. Other persons must be denied access to the internal reporting channel. With the consent of the persons concerned, their identity may also be disclosed to other persons. Exceptions exist, for example, for the disclosure of identity in connection with criminal proceedings.

Dealing with reports and taking follow-up action

Whistleblowers must be given an acknowledgement of receipt within seven days of receipt of the report. Within three months of confirmation of receipt, whistleblowers must then be provided with information on any follow-up measures planned or already taken, as well as the reasons for such measures. Follow-up measures include, in particular, the initiation of internal investigations, the referral of the whistleblower to other competent bodies, the closure of the proceedings due to insufficient evidence or for other reasons, or the transfer of the matter to a competent authority. In addition, it is of course also conceivable to take measures to directly eliminate any violations.

Incoming reports must be documented in a manner that preserves confidentiality. The documentation must be deleted three years after completion of the procedure. Longer retention is permissible if this is necessary and appropriate for the fulfilment of the requirements of the HinSchG, or under other legal provisions.

Whistleblower protection

Whistleblowers are generally protected against reprisals. This also includes the mere threat and attempt to take reprisals. In connection with employment relationships, for example, dismissals, demotion or exclusion from promotion, intimidation, harassment, refusal to extend fixed-term employment contracts or giving negative performance appraisals are prohibited. If reprisals occur, there is the threat of severe fines. In addition, companies are obligated to pay damages; however, compensation for immaterial damages (i.e., damages for pain and suffering) is excluded.

In order to provide whistleblowers with even greater protection, a reversal of the burden of proof applies. If an alleged disadvantage occurs after a report has been submitted and the whistleblower claims that it is a case of reprisal, the company must explain and, if necessary, prove the (alternative) reason for the alleged disadvantage.

However, whistleblowers are only protected against reprisals if the subject of the report falls within the scope of the HinSchG, the report is not submitted in a grossly negligent or even intentionally false manner, and the official reporting channels are used.

Conversely, whistleblowers who submit a false report due to gross negligence or intent are obliged to compensate the person concerned for the damage resulting from the false report.

Fine risks

Violations of material provisions of the HinSchG can usually result in fines in the range of EUR 10,000 to 50,000. Under certain circumstances, however, companies may also be subject to fines of up to EUR 500,000. Companies that fail to comply with an obligation to set up and operate an internal reporting office, for example, face a fine of up to EUR 20,000. However, this fine will not come into force until 1 December 2023, so companies that have already been required to set up and operate an internal reporting office since July 2, 2023 still have some room to maneuver.

Conclusion and outlook

Companies would be well advised to clarify quickly whether they are obliged to set up an internal reporting office on the basis of the HinSchG. Existing whistleblowing systems may need to be adapted, in particular to meet the increased requirements for confidentiality and documentation. Appropriate instructions must be drawn up for reporting channels on how to deal with incoming reports. When setting up a company's own reporting channel (i.e., without outsourcing to third parties), it must be ensured that the personnel deployed are independent and sufficiently qualified. In addition to the data privacy officer, other departments must also be involved (e.g., Legal and Compliance) so that processes are set up in compliance with the law. The reversal of the burden of proof in the event of an allegation of reprisals should definitely be taken into account in significant personnel-related decisions. ←

ADVERTISEMENT

Frankfurter Allgemeine Konferenzen Produkthaftung und Produktsicherheit

27.–28.9.2023
F.A.Z. Tower, Frankfurt am Main



Bleiben Sie auf dem neuesten Stand bei Themen wie:

- Herausforderungen durch die neue Produkthaftungsrichtlinie wie Software als Produkt, Discovery in Europa, Beweiserleichterungen für Geschädigte, Wegfall der Haftungshöchstgrenze
- der neuen Produktsicherheitsverordnung und Maschinenverordnung
- dem neuen Rechtsrahmen aus der KI-Verordnung und der KI-Haftungsrichtlinie, Regulatory Sandboxes und Klassifizierungstaxonomie
- Product Compliance und die Auswirkungen des Green Deals
- RAPEX, Rückrufe, Mystery Shopping etc. – erste Erfahrungen mit der neuen Marktüberwachungsverordnung

Sprecher u.a.:



© Annika List Fotografie
Prof. Dr. Roman Poseck
Hessischer Minister
der Justiz



Dr. Amaryllis Verhoeven
European Commission



Dr. Jean Obst
Robert Bosch GmbH



Dr. Christian Piovano
ZF Friedrichshafen AG

Initiatoren



Medienpartner



Anmeldung und weitere Informationen finden Sie unter
www.faz-konferenzen.de/produkthaftung-und-produktsicherheit. Wir freuen uns auf Sie!