



The German Whistleblower Protection Act – FAQ

As at May 2023

The Whistleblower Protection Act (HinSchG) has been passed. The purpose of the Act is to protect whistleblowers from disadvantages in the future. Companies with more than 249 employees must set up and operate a whistleblower system after the Act comes into force (expected in June 2023). Otherwise, there is the risk of a heavy fine and the legal leakage of critical company information and know-how.

As from 17 December 2023, this obligation will also apply to companies with at least 50 employees.

We have compiled alphabetically the most important questions from the point of view of the respective compliance/legal/human resources department. However, caution is required when dealing with compliance issues, as it always depends on the individual case. Legal advice is just as necessary when dealing with whistleblowers as ensuring confidentiality in the whistleblowing process. The FAQs are no substitute for an examination of the legal situation in the individual case and do not constitute legal advice.

Our whistleblowing experts Dr. Oliver Bertram, Isabel Bäumer, Mareike Gehrman, Dr. Martin Knaup, Dr. Rebekka Krause and Jan-Patrick Vogel, LL.M., can be contacted as indicated:

Whistleblowing Hotline:

+49 69 97130-283

Whistleblowing Task Force:

whistleblowing@taylorwessing.com

Webinars/Info:

Further information and webinar options can be found at taylorwessing.com/en/insights-and-events/insights/whistleblowing

Keyword	Question	Answer
<p>Anonymity</p> <p>A</p>	<p>Does the whistleblower system have to allow anonymous reports or do they have to be processed by the company?</p>	<p>The internal reporting office should also process incoming reports anonymously. However, there is no obligation to design the reporting channels in such a way that they allow anonymous reports to be submitted.</p> <p>The external reporting office should also process anonymous incoming reports. Subject to special legal regulations, however, there is no obligation to design the reporting channels in such a way that they enable anonymous reports to be submitted.</p>
<p>Central whistleblowing system</p> <p>C</p>	<p>Are central whistleblower systems still permissible in groups of companies and corporations?</p>	<p>According to the previous opinion of the EU Commission, a group-wide central whistleblower system at the parent company does not constitute a permissible allocation of resources. This means that subsidiaries that fall within the scope of application due to their number of employees must (additionally) set up their own decentralised whistleblowing system.</p> <p>The HinSchG expressly advocates a so-called “group privilege”, i.e. group-wide reporting offices remain permissible. According to this, the internal reporting office of a company can not only be “outsourced” to law firms, for example, but an independent and confidential office can also be established centrally within a group of companies as a third party within the meaning of Section 14 (1) HinSchG. In this context, it is necessary that the original responsibility for following up and remedying an identified violation always remains with the respective group company commissioning the work. Easy access must be guaranteed for persons providing information (e.g. no language barriers).</p> <p>Considering the contradiction between the HinSchG and the EU Commission's view, it is advisable to critically question the admissibility of group-wide hotlines.</p>
<p>Company externals</p>	<p>Does the whistleblower system also have to be opened up to external parties?</p>	<p>The HinSchG does not impose an obligation on companies to accept information from persons who do not fall within the personal scope of application, i.e. from outside the company. However, it is advisable to consider this as an option, especially with regard to the obligation to set up a complaints procedure provided for in the Supply Chain Due Diligence Act.</p>

Keyword	Question	Answer
<p>Compliance Management System</p>	<p>Does a whistleblower system need to be integrated into a company's compliance management system (CMS)?</p>	<p>A functioning whistleblower system is a central component of an effective CMS and must therefore be linked to the other elements of a CMS. In addition to identifying compliance violations, the whistleblower system also serves to determine whether the preventive compliance measures taken are effective and whether any misconduct is avoided. To the same extent, a whistleblower system helps to identify necessary adjustments and improvements to the CMS and, at the same time, to preserve the authority to interpret the facts underlying the respective report in favour of the company concerned.</p>
<p>Confidentiality</p>	<p>Are the persons providing the information and the persons named in the report to be treated confidentially in the company?</p>	<p>Yes, the HInSchG requires reporting channels to be securely designed, set up and operated in such a way that the confidentiality of the identity of the whistleblower and third parties mentioned in the report is maintained and unauthorised employees are denied access to them.</p> <p>However, the HInSchG regulates exceptions according to which the requirement of confidentiality does not apply in certain cases (e.g. the identity of a person who intentionally or grossly negligently reports false information is not covered by the protection of confidentiality).</p> <p>It is also recommended that all staff members authorised to receive and/or process whistleblowing notifications sign a separate confidentiality agreement.</p>


Keyword	Question	Answer
<p>Data protection</p>	<p>From a data protection point of view, what aspects need to be taken into account, especially when using web-based whistleblowing systems?</p>	<p>When processing personal data, the internal reporting unit shall comply with the rules on data protection. Insofar as the FIU processes personal data in order to perform the tasks within its competence, especially in the case of FIUs operated by an individual, the individual shall not be the data controller within the meaning of the data protection regulations.</p> <p>The legal basis for the processing of personal data is Art. 6 para. 1 lit.c GDPR in conjunction with Section 10 HinSchG. The standard also includes the processing of special categories of personal data from Art. 9 GDPR. When processing special categories of personal data for the purposes mentioned in the first sentence, the notification office must provide for appropriate and specific measures to protect the interests of the data subject. Section 22(2) sentence 2 of the Federal Data Protection Act shall be applied accordingly.</p> <p>The legal basis should be sufficiently documented. In addition, complete information about the data processing pursuant to Arts. 13 and 14 GDPR is required and, as a rule, this must be provided to all persons whose personal data is processed. Furthermore, a data protection impact assessment must be carried out as part of the implementation.</p> <p>If external third parties are commissioned to set up and operate the internal notification office, the requirements for commissioned data processing must be observed, see Art. 28 of the GDPR. If processing also takes place outside the EU or the EEA (even if it is only access for support purposes to data in the EU), further safeguards are required to ensure an adequate level of data protection. If the whistleblower system violates these or other data protection requirements, serious sanctions may be imposed.</p>
<p>Disclosure</p>	<p>Are whistleblowers allowed to go public with sensitive company information?</p>	<p>A whistleblower who discloses information to the public can only invoke the whistleblower protection if the company (internal) and/or the authority (external) have not taken appropriate measures within the timeframe provided for or, in exceptional cases, if there is sufficient reason to believe that the public interest is at risk, there is a fear of reprisals or there is no prospect of clarification.</p> <p>The HinSchG therefore also protects, as an extreme possibility, the submission of indications to the public, e.g. via social media or to the law enforcement authorities.</p>



Keyword	Question	Answer
Documentation obligation	Which time period is obligatory for the documentation and how should the documentation be carried out?	The persons responsible for receiving reports at a reporting office shall document all incoming reports in a permanently retrievable manner in compliance with the confidentiality requirement. If the report is made by telephone or other means of voice transmission, a usable audio recording of the conversation may only be made with the consent of the person making the report. The documentation shall be deleted three years after completion of the procedure. The documentation may be kept longer to meet the requirements of the HinSchG or other legislation, as long as this is necessary and proportionate.
Employee	Which persons are allowed to submit reports via the company's internal whistleblowing system?	The HinSchG stipulates that the reporting channels must be open to all employees of the company. The term "employee" is interpreted broadly (including executive employees, trainees, temporary workers, persons similar to employees and management bodies). Civil servants are also included. In addition, the reporting channels can also be opened for other persons (cf. statements on "Company externals").
External reporting office	What is an external reporting office? Are whistleblowers also allowed to contact external external reporting office directly?	<p>An external reporting office is an authority to which information about misconduct can be reported verbally or in writing.</p> <p>The whistleblower may choose whether to first contact the company internally and/or the competent authority externally. These persons should prefer to report to an internal reporting office in cases where effective action can be taken against the violation and they do not fear reprisals.</p> <p>A central external reporting office is to be established at the Federal Office of Justice (BfJ). In addition, the existing reporting systems at the Federal Financial Supervisory Authority (BaFin) and the Federal Cartel Office (Bundeskartellamt) are to be continued as further external reporting offices with special responsibilities.</p> <p>Companies should intensively support an internal whistleblowing system in order to create the greatest possible incentives for this to be used as a matter of priority and to therefore avoid external whistleblowing as far as possible. Companies shall provide clear and easily accessible information to employees on the use of the internal reporting procedure. This must not restrict or impede the possibility of making an external report.</p>

Keyword	Question	Answer
<p>False reports</p>	<p>What are the consequences of a false report?</p>	<p>A false suspicion in the context of a report or disclosure can have far-reaching consequences for those affected. The effects may no longer be completely reversible. Therefore, the injured parties are entitled to compensation for the damage resulting from an intentional or grossly negligent false report or disclosure.</p> <p>Furthermore, the identity of persons who intentionally or grossly negligently report false information is not protected from disclosure under the HinSchG. In the event of such a false report, persons who are the subject of this report have a legitimate interest in obtaining knowledge of the identity of the reporting person in order to be able to assert claims for damages if necessary.</p>
<p>Feedback requirement</p>	<p>Is the company obliged to give feedback to the whistleblower?</p>	<p>The whistleblower should be informed as comprehensively as possible about the handling of his or her whistleblowing. This includes both an acknowledgement of receipt and an explanation of the follow-up measures planned and taken as well as the results of any investigation.</p> <p>Within a period of 7 days after receipt of a report, the person making the report must be given confirmation of receipt. Within a reasonable time frame – maximum 3 months – the whistleblower must be given feedback on follow-up measures.</p>
<p>Internal reporting office</p>	<p>What is an internal reporting office and who in the company can perform this function?</p>	<p>An office within a legal entity in the private or public sector to which information about misconduct can be communicated verbally or in writing, in particular a manager, compliance officer, HR manager, ombudsperson (e.g. lawyers), company employee representative. For better handling of a whistleblowing system, the department/person who performs the function of internal reporting office in the company should be explicitly entrusted with this responsibility.</p>
<p>International whistleblower system</p>	<p>Can the whistleblower system of the parent company abroad be used for subsidiaries and sub-subsidiaries abroad?</p>	<p>If the data protection requirements for a cross-border data transfer have been met, the whistleblower system of the parent company can only be used as an additional tool. The subsidiaries and sub-subsidiaries must also maintain a local reporting channel (cf. statements on the “Central whistleblowing system”).</p> <p>Companies should intensively support an internal whistleblowing system in order to create the greatest possible incentives for this to be used as a matter of priority and to therefore avoid external whistleblowing as far as possible. Companies shall provide clear and easily accessible information to employees on how to use the internal reporting procedure. This must not restrict or impede the possibility of making an external report.</p>

Keyword	Question	Answer
IT Department	Can my company's IT department have access to the whistleblower system for IT support and to ensure IT security?	According to the HinSchG, only authorised employees who are responsible for receiving reports or for taking follow-up action on reports may have access to information that reveals the identity of the whistleblower. As a rule, however, the IT department is not responsible for receiving and clarifying reports, so the IT department must be shielded from the content of any reports.
Know-How Protection	Can business secrets and/or confidential information of the company also be reported via the whistleblower system?	<p>Whistleblower protection cannot be obtained for all reports or disclosures.</p> <p>Security interests as well as confidentiality and secrecy obligations take precedence over the HinSchG (e.g. Confidentiality obligations of lawyers, notaries or doctors and pharmacists).</p> <p>However, there are cases in which protection under the HinSchG exists despite existing duties of confidentiality or secrecy. For this to be the case, the person providing the information must have reasonable grounds to believe that the report or disclosure is necessary to uncover a violation.</p> <p>Persons who have acquired trade secrets or confidential information in a professional context therefore only enjoy protection under the HinSchG if they meet the requirements of this Act and the disclosure of the trade secret was necessary to uncover an infringement within the material scope of this Act. The disclosure of trade secrets or confidential information is therefore permitted.</p>
Ombudsperson system	What is an ombudsperson system? May external ombudspersons continue to be used as "reporting offices"?	<p>An ombudsperson system usually involves external lawyers who are available as a contact point for whistleblowers. These lawyers pass on the information to the company, after carrying out a legal "first level check".</p> <p>The establishment of an ombudsperson system continues to be a permissible reporting channel.</p>
Protection of accused persons	Do the persons accused by the whistleblower also have to be protected by the company?	The HinSchG requires reporting channels to be designed, set up and operated in such a secure manner that not only the confidentiality of the identity of the whistleblower but also that of third parties mentioned in the report is maintained and unauthorised employees are denied access to it. In particular, balancing the protection of the accused on the one hand and the protection of whistleblowers on the other hand often causes problems in internal company investigations.

Keyword	Question	Answer
Public sector	Does the public sector also need to introduce whistleblowing systems?	<p>Yes, the obligation to establish internal reporting channels and procedures for internal reporting and follow-up applies to legal entities in the private and public sectors. For municipalities and associations of municipalities and such employment providers that are owned or controlled by municipalities and associations of municipalities, the obligation to establish internal reporting bodies is governed by the respective national law.</p> <p>In addition, some of the obligations of the EU Whistleblower Directive do not only exist from the entry into force of the HinSchG, but already since 18 December 2021. At the latest, all whistleblower protection obligations for the public sector take effect from the entry into force.</p>
Reprisals	Which measures constitute reprisals within the meaning of the HinSchG?	<p>Reprisals refers to any direct or indirect action or omission in a professional context, triggered by an internal or external report or disclosure, which may cause unjustified disadvantage to the whistleblower (e.g. dismissal or suspension, warning, transfer or reassignment, failure to receive promotion, failure to receive training, social exclusion, mobbing, etc.).</p> <p>In the event of a violation of the prohibition of reprisals, the perpetrator is obliged to compensate the whistleblower for the resulting damage.</p>
Reversal of the burden of proof	Who bears the burden of proving that a company has taken unlawful measures under employment law against a whistleblower?	<p>If a whistleblower suffers a disadvantage in connection with his or her professional activities and claims to have suffered such disadvantage as a result of a report or disclosure under this Act, such disadvantage shall be presumed to be a reprisal for such report or disclosure. This means that in such cases the employer must prove that its actions were in no way connected to the report or disclosure made (reversal of the burden of proof).</p> <p>However, the whistleblower must demonstrate and prove that a measure constitutes a disadvantage.</p>
Risks	What are the risks for companies that have not implemented a whistleblowing system?	<p>Failure to establish or operate an internal reporting system may result in a fine. In addition, there is of course the risk of a (legitimate) outflow of know-how due to public reports (especially of business secrets) as well as a risk of reputational damage (cf. "Sanctions").</p>

Keyword	Question	Answer
<p>Sanctions</p> 	<p>What sanctions are imposed on the company if the requirements of the HinSchG are not implemented?</p>	<p>Preventing a report and the subsequent communication, taking a prohibited reprisal or intentionally or recklessly disregarding the confidentiality requirement is punishable by a fine of up to EUR 50,000. The negligent breach of the confidentiality requirement is punishable by a fine of up to EUR 10,000. Companies that do not comply with their obligation to set up and operate an internal reporting office face a fine of up to EUR 20,000.</p> <p>The reference to Sections 30 and 130 Administrative Offences Act makes it possible that the maximum limit for fines can be increased tenfold in the case of serious violations.</p>
<p>Scope of application</p>	<p>What is the scope of application of the HinSchG?</p>	<p>The personal scope of application of the HinSchG is broad and includes all persons who have obtained information about violations in connection with their professional activities. In addition to employees (cf. statements on “Employee”), this may also include civil servants, self-employed persons, shareholders or employees of suppliers.</p> <p>The material scope of application shall include in particular all violations which are punishable by law, as well as violations subject to fines, insofar as the violated regulation serves to protect life, limb, health or the rights of employees or their representative bodies (e.g. occupational health and safety, health protection). In addition, all violations of legal norms that were adopted to implement European regulations are included (extended to a limited extent to national regulations from the respective regulatory area).</p>
<p>Transparency</p> 	<p>How can company employees know whether they should report observed or experienced conduct in the whistleblowing system?</p>	<p>It is often not easy for employees to assess whether behavior they have experienced is considered a violation of the law” or “unethical conduct. It is therefore advisable to use clearly formulated policies and guidelines to give employees an unambiguous picture of what conduct is considered worthy of reporting. Complex legal terms should be avoided as far as possible. The same applies to the communication of a transparent understanding of the responsibilities and processes for handling incoming reports in order to gain and maintain the trust of employees in the functioning and effectiveness of a whistleblowing system. To this end, accurate information should be provided to potential whistleblowers in an easily accessible manner. It is therefore recommended that the whistleblowing process be recorded in a guideline/policy (unless a works council agreement is to be concluded anyway) and handed out to all employees.</p>

Keyword	Question	Answer
Violations 	What violations can be reported in accordance with the HinSchG?	According to the scope of the EU Whistleblower Directive, only the reporting of violations of certain EU law is subject to its protection. The HinSchG expands the scope of application and includes violations of national law. Violations of criminal law, violations that are subject to fines, insofar as they serve to protect life or health or to protect the rights of employees or their representative bodies, as well as all violations of federal and state law fall within the material scope of the HinSchG.
Whistleblower 	Who can be the whistleblowing person in the company?	A whistleblower can be any natural person to whom the reporting channel is open, i.e. any employee of the company and, if applicable, including external persons, and who reports or discloses information on violations obtained in connection with his or her work activity (cf. statements on "Employee", "Scope of application" and "Company externals").
Whistleblower protection	What measures must the company take to protect the whistleblower?	It is a core obligation for companies to (i) protect whistleblowers from reprisals of any kind, direct or indirect, including threats and attempts to do so, and (ii) maintain the confidentiality of whistleblowers' identities. There is extensive protection against reprisals.
Works Council	What role does the works council play in the implementation of a whistleblower system and the clarification of reports?	As a rule, the works council has a right of co-determination in the implementation of a whistleblower system, i.e. the whistleblower system may not be introduced without the prior consent of the works council. In groups of companies, the competence of the group works council, the central works councils and/or the local works councils must be carefully examined and, in case of doubt, delegation resolutions must be sought.

Whistleblowing hotline: +49 69 97130-283

Whistleblowing Task Force: whistleblowing@taylorwessing.com

Webinars/Info: Further information and offers for webinars can be found at taylorwessing.com/en/insights-and-events/insights/whistleblowing