



**WHISTLEBLOWER PROTECTION ACT:
WHAT COMPANIES MUST DO**



With the so-called Whistleblower Protection Act, the German legislator has implemented the EU's Whistleblower Directive into German law in May 2023. The Whistleblower Protection Act has been in force for larger companies with 250 or more employees since June 2023. Smaller companies with 50 or more employees must comply with the provisions of the Act since December 17, 2023.

WHICH COMPANIES ARE CONCERNED?

The Whistleblower Protection Act prescribes the implementation of a whistleblower system. This generally affects all private and public law companies with regularly at least 50 employees.

Section 12 (3) of the HinSchG (Whistleblower Protection Act) mandates the obligation for certain companies regardless of their number of employees. This particularly affects companies in the financial services sector.

RELIEF FOR MEDIUM-SIZED COMPANIES...

Certain reliefs exist only for medium-sized companies with a workforce of 50 to 249 employees. These companies may establish and operate a joint office for receiving reports and for further measures, according to Section 14 (2) HinSchG. However, they remain individually obligated to remedy the violation and to provide feedback to the whistleblower.



...AND GROUP COMPANIES

For group companies, there is relief as far as an independent and confidential office as a “third party” can be established at another group company, which can also be active for several independent companies within the group.

Internal reports must also be possible in the working language prevailing in the respective commissioning subsidiary. The appointment of a central reporting office at a group company must not create additional barriers for whistleblowers.

WHAT TYPES OF WHISTLEBLOWER SYSTEMS ARE POSSIBLE?

Section 7 of the HinSchG (Whistleblower Protection Act) essentially provides for two equally valid reporting channels for whistleblowers – an internal and an external reporting channel. It is legally prescribed that the whistleblower should prefer reporting to an internal reporting channel in cases where the violation can be effectively addressed internally and they do not fear reprisals, according to Section 7 (1) sentence 2 HinSchG.

Internal Reporting Channel

There is flexibility in the precise design of the company-internal reporting channel. The internal reporting office can be established by:

- > an individual employed by the respective employer,
- > a work unit consisting of several employed persons, or
- > a third party

being entrusted with the tasks of the internal reporting office. This means that also a lawyer can act as an external ombudsperson to take on the tasks of the internal reporting channel. In any case, the person concerned needs sufficient competencies to be able to carry out the necessary legal assessment of the reports.

The tasks of the internal reporting office include operating the reporting channels, conducting the legally prescribed procedure for internal reports (Section 17 HinSchG) and taking appropriate follow-up measures.

The reporting channels must be designed in such a way that reports can be made in written or oral form.

When a whistleblower report is received by the company, the confidentiality of the identity of the whistleblower, the persons who are the subject of the report and other persons mentioned in the report must be maintained, according to Section 8 HinSchG.

Exceptions to this confidentiality requirement exist only in very limited cases, according to Section 9 HinSchG.

Note: An obligation to establish reporting offices that also allow anonymous reporting, which was envisaged during the legislative process, no longer exists according to the now-enacted law. Section 16 (1) sentence 4 HinSchG merely provides that the internal reporting office should also process anonymously received reports. Companies are free to enable anonymous contact and anonymous communication between the whistleblower and the internal reporting office. This applies in particular for those who have already established such channels.

Particularly suitable as whistleblower system is the establishment of an electronic reporting option. However, upon the whistleblower's request, a physical meeting must also be made possible within a reasonable timeframe, according to Section 16 (3) HinSchG.

Note: The possibility for whistleblowers to have a personal conversation is particularly important when entrusting a third party with the tasks of an internal reporting office. With the consent of the whistleblower, however, the meeting can also take place via video and audio transmission, according to Section 16 (3) HinSchG.

The internal reporting channel must be open to at least the employees and temporary workers of the company. Voluntarily, the whistleblower system can also be made accessible to those who get into contact with the respective company within scope of their professional activity. This includes, for example, company officers and shareholders, applicants, self-employed individuals or former employees.

External Reporting Channels

In addition to establishing an internal reporting system, companies must also provide their employees as potential whistleblowers, with understandable and easily accessible information about the possibilities of external reporting to certain authorities.

Note: For external reporting offices, too, they should process anonymous reports, but they do not have to establish a corresponding channel for this purpose, according to Section 27 (1) HinSchG.

At the same time, Section 24 (2) HinSchG sees a task of the external reporting offices in informing about the possibility of an internal report.

The whistleblower can basically decide whether to report violations internally to the company or to contact an external authority. However, as stated above, internal reporting offices should be preferred, according to Section 7 (1) HinSchG.

According to Section 7 (3) HinSchG, employers should create incentives for whistleblowers to contact the respective internal reporting office before reporting to an external reporting office and provide clear and easily accessible information to employees about the use of the internal reporting procedure. At the same time, they are obliged to inform about external reporting procedures according to Section 13 (2) HinSchG.

WHICH WHISTLEBLOWER-REPORTS ARE PROTECTED?

The Whistleblower Protection Act extends its scope beyond the requirements of the EU-Directive. Whistleblowers are protected when reporting violations that are punishable by criminal law or (with some restrictions) by fines, according to Section 2 (1) No. 1 and 2 HinSchG. The report must contain information about violations in the employer's company where the whistleblower is or was active, or at another entity with which the whistleblower is or was in contact due to his professional activity, according to Section 3 (3) HinSchG.

Furthermore, the substantive scope of application extends to other violations of federal and state legal provisions as well as directly applicable legal acts of the EU and the European Atomic Energy Community, according to Section 2 (1) No. 3 to 10, (2) HinSchG. This includes, among others, the following areas:

- > combating money laundering and terrorist financing,
- > product safety and conformity,
- > traffic safety including railway safety, maritime traffic, and air traffic safety,
- > environmental protection,
- > radiation protection and nuclear safety,
- > food and feed safety, animal health and welfare,
- > public health,
- > consumer protection,
- > protection of privacy and personal data as well as the security of network and information systems,
- > certain violations of the Act Against Restraints of Competition (GWB).

IMPLEMENTATION OF THE WHISTLEBLOWER PROTECTION ACT IN THE COMPANY

Companies are well advised to ensure internal processes in the event of an internal report. These should be set out in a whistleblower policy, possibly also in a Code of Conduct, and communicated accordingly. Employees should be encouraged to report primarily to the internal reporting office to avoid potential damage to their reputation.

Appointment of Contact Persons

Independent (compliance) contact persons must be appointed for internal reports. Both internal employees and external third parties are eligible. If companies operate the internal reporting office with their own employees, the staffing of the reporting office must be ensured and the relevant personnel must be trained, especially in compliance. The responsible employees must be able to legally check whether the notification is reportable according to the HinSchG and meet the high requirements for the confidential handling of the report.

Note: Employers should document corresponding qualifications and be able to provide them if necessary. It is also important to ensure the independence of the responsible employees and to be able to exclude conflicts of interest. If companies organize the internal reporting office through external ombudspersons, such as lawyers, they can rely on their qualifications.

Involvement of the Works Council

If a works council exists in the company, it should be involved early and appropriately in the implementation of a whistleblower system. Specifically, the works council must be informed in advance about the planned establishment of a whistleblower system, according to Section 80 (2) BetrVG (Works Constitution Act). Its implementation can release a right of co-determination from Section 87 (1) No. 1 BetrVG, according to which the works council has to be included in matters of the organization of the company and the behavior of employees in the company.

Although there is no co-determination right of the works council regarding the decision on "whether," i. e., whether an internal reporting office is to be established, given the existing legal obligation, there are design options regarding the specific design of the whistleblower system or the appointment of the internal employees operating the internal reporting office, in which the works council must be involved, according to Section 99 BetrVG.

Accordingly, the decision on whether the company sets up the internal reporting office within the company itself or with an external third party is not subject to co-determination.

The further procedure regarding the processing of received notifications also offers scope for the co-determination rights of the works council.

Finally, the works councils must be properly involved in any training measures that become necessary due to the establishment and operation of an internal reporting office, according to Sections 96 et sqq. BetrVG.

Compliance with Legal Requirements for Processing Internal Reports

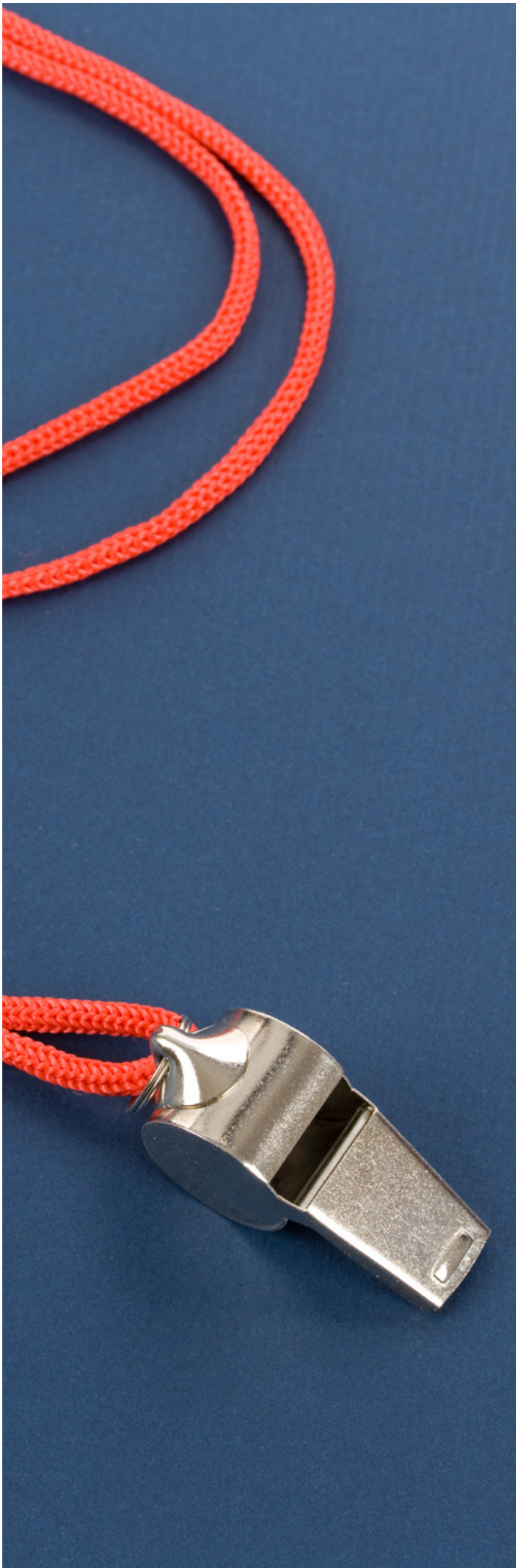
The process after receiving a notification is legally prescribed. It is advisable to create a written action plan to maintain feedback deadlines and confidentiality. The following steps must be observed:

1. The whistleblower must receive confirmation of receipt of the report within seven days.
2. The received notification must then be checked by the internal reporting office.
3. Incoming reports must be documented, according to Section 11 HinSchG. If necessary, the documentation should be presented to the whistleblower for verification.
4. Appropriate follow-up measures must be taken, according to Section 18 HinSchG.

Note: For the conduct of internal investigations – while maintaining confidentiality – information can also be passed on to work units within the company, according to Section 18 No. 4 HinSchG.

5. The internal reporting office must provide feedback to the whistleblower within three months after confirming receipt of the report. The feedback includes notification of planned and already taken follow-up measures as well as the reasons for them.





Note: The extent to which employers should create incentives to use internal reporting procedures first is not specified by the law. Since the whistleblower should prefer internal reporting channels if no retaliation is to be feared and it is expected that effective action will be taken against the violation, this can be seen as an explicit appeal by the legislator for corresponding professional internal structures. Only if whistleblowers can trust that companies take notifications seriously, investigate them carefully and clarify crimes or irregularities as well as sanction them appropriately, will they prefer these internal reporting structures as intended.

Reporting and Notification Obligations of the Employer?

To effectively punish or remedy violations and to act in compliance with the law, employers must observe any reporting and notification obligations in other laws.

With certain exceptions (Section 138 of the German Criminal Code), criminal offenses are generally not subject to mandatory reporting. However, in the case of tax law violations, there may be an immediate obligation to correct the tax declaration according to Section 153 of the German Fiscal Code (AO), the violation of which can lead to criminal liability for tax evasion. Further reporting obligations may arise from the Money Laundering Act.

In some cases, proactive contact with investigative authorities may be advisable to reduce the risk of timely alternative knowledge by the authorities, such as through external reporting offices. This can also serve to avert impending coercive measures and to limit the risk of one's criminal liability, possibly due to omission.

Furthermore, a functioning compliance system requires a clear commitment to lawful behavior, which in turn can be ensured by filing a criminal complaint. If the filing of a criminal complaint is considered, the three-month application period for so-called application offenses must be observed.

PROTECTION FOR THE WHISTLEBLOWER

Whistleblowers are only legally protected if there was a justified reason to believe that the reported information about violations was true at the time of the report, fell within the scope of the law and was submitted via the prescribed internal or external reporting channels.

In this case, the HinSchG then prohibits any reprisals against whistleblowers, according to Sections 33 et seq. HinSchG. Thus, whistleblowers must not fear any labor law consequences for a proper report: for example, they must not be subject to dismissal, non-consideration for a promotion opportunity, transfer, or denial or reduction of a bonus. To effectively design this prohibition of retaliation, whistleblowers can rely on a reversal of the burden of proof, according to Section 36 (2) HinSchG. Accordingly, the existence of retaliation is legally presumed and the employer must refute this presumption. In the event of a violation of the prohibition of retaliation, there is a claim for damages for financial losses of the whistleblower.

Note: In this context, companies should document the foundations and motives of personnel decisions well..

For violations of the HinSchG, sanctions with substantial fines between 10,000 and 50,000 euros are provided, according to Section 40 HinSchG. Fines for not establishing a corresponding internal reporting office will only be imposed after a transition period of six months from the applicability of the regulations.

The fines can affect both the responsible individuals and (via Section 30 of the German Regulatory Offenses Act) the respective companies. For certain violations, the fine against the company can also increase tenfold, according to Section 40 (6) sentence 2 HinSchG.

CONCLUSION

Companies with 50 or more employees must implement a whistleblower system and comply with the legal requirements regarding the necessary processes and recording obligations.

To avoid potential damage to reputation, companies should transparently design the internal reporting channel in their own interest and employees should be fully informed about the use of this internal whistleblower system. In addition, a company-internal whistleblower policy should be implemented or embedded in a Code of Conduct.

CONTACT PERSONS

Our experts on the EU Whistleblower Directive are available to answer any questions you may have.



Dr. Sven Christian Gläser

Lawyer, tax consultant
and partner
at RSM Ebner Stolz Stuttgart
T +49 (0)711 2049-1411
sven.glaeser@ebnerstolz.de



Philipp Külz

Lawyer, specialised lawyer for tax
law, certified counselor for criminal
tax law (DAA) and partner
at RSM Ebner Stolz Cologne
T +49 (0)221 20643-417
philipp.kuelz@ebnerstolz.de



Dr. Detlev Heinsius

Lawyer, specialised lawyer
for tax law and partner
at RSM Ebner Stolz Hamburg
T +49 (0)40 37097 -174
detlev.heinsius@ebnerstolz.de



Christina Odenthal-Middelhoff

Lawyer, certified consultant for criminal
tax law (DAA) and partner
at RSM Ebner Stolz Cologne
T +49 (0)221 20643-499
christina.odenthal@ebnerstolz.de

Publisher

RSM Ebner Stolz
Wirtschaftsprüfer Steuerberater Rechtsanwälte Partnerschaft mbB

Legal status: 27.05.2024

Editorial office

Dr. Ulrike Höreth, T +49 (0)711 2049-1371
Brigitte Stelzer, T +49 (0)711 2049-1535

This publication contains only general information which cannot be used suitable for basing decisions on in individual cases. The publisher and the authors do not assume any liability for the correctness and completeness of the information. Should the reader of this publication consider the information contained therein to be relevant for themselves, it is their sole responsibility or that of their advisors to ensure that the information is factually correct to verify; in no event shall the foregoing information be construed to be in no way suitable as a substitute for competent advice in individual cases. The publisher is at your disposal for this purpose.

The information is subject to copyright protection. Storage for one's own private purposes or forwarding for private purposes (in complete form only) is permitted. Commercial exploitation, in particular the (even partial) reprint in other newsletters or the publication on websites, require the consent of the publishers.

The RSM Ebner Stolz group companies are members of RSM network and trade as RSM. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

© RSM International Association, 2024

THE POWER OF UNDERSTANDING
ASSURANCE | TAX | CONSULTING | LEGAL

