The Whistleblower Directive of the EU

Ulrich Herfurth, attorney at law in Hanover and Brussels
Sara Nesler, Mag. iur. (Torino), LL.M. (Münster), Hanover

September 2023

Companies in Europe must prepare for another compliance requirement: the EU's so-called *Whistleblower Directive* should have been implemented by December 2021. Although there were significant delays in most countries, the corresponding laws have entered into force in all member states now, except Poland and Estonia. The aim of the Directive is to create a comprehensive system of protection for whistleblowers when they uncover misconduct in companies and institutions. To achieve this, companies with 50 or more employees will be required to set up internal reporting channels. The immediate provision of internal reporting channels is necessary to avoid possible fines and investigations through reports to external channels.

This paper is based on the German implementation of the Whistleblower Directive, the *Hinweisgeberschutzgesetz* (HinSchG), but similar rules apply in the other member states.

Scope

The Whistleblower Directive mandates the protection of reports of EU law breaches, for example breaches of product safety and consumer protection. It encourages member states to extend the scope by law, and the German legislator has made use of this option. It covers, among other things, reports of criminal offences and administrative offences, insofar as the violated regulation serves to protect life, body or health, or to protect the rights of employees or their representative bodies.

Trade secrets

Reports and disclosures of information containing trade secrets are particularly problematic. Trade secrets and information subject to a contractual duty of confidentiality may only be reported or disclosed pursuant to Section 6 HinSchG if the whistleblower had sufficient reason to believe that the transfer or disclosure of the information was necessary to uncover a breach. However, the suitability of the disclosure for the protection of the general public interest is not required, unlike in Section 5 of the German Trade Secrets Protection Act, so-called *Geschäftsgeheimnisgesetz* (GeschGehG).

Protected persons

The HinSchG protects current and former employees as well as trainees, civil servants, and persons like employees who obtain information about breaches in the course of professional, entrepreneurial or official activities or in the run-up to such activities and report them to the designated reporting channels or, exceptionally, disclose them. In addition, persons who

support whistleblowers, for example journalists, are also protected.
However, the protection only applies if, at the time of the report or disclosure, the whistleblower had reasonable grounds to believe that the information he reported or disclosed was true and that the information reported concerned breaches falling within the scope of the Directive. The motivation of the whistleblower is irrelevant. The HinSchG, on the other hand, does not protect intentional or grossly negligent disclosure of false information, but establishes a claim for damages by the company.

Reporting channels

According to the HinSchG, whistleblowers can choose to use an internal reporting channel or an external reporting channel. Internal channels are those established by companies and concerned institutions, even if they commission a third party with the task. External channels are established at selected authorities at federal and state level.
The German legislator emphasises that whistleblowers "should" prefer internal reporting channels if effective internal action can be taken against a breach and no reprisals are to be feared. However, this open wording does not establish an obligation, especially since the lack of "fear of reprisals" would be difficult to prove in the event of a dispute. Nevertheless, it remains important for companies to immediately set up a reporting channel that is trustworthy for employees - otherwise the path to an external reporting channel is favoured in any case, with unforeseeable consequences. Disclosure to third parties, on the other hand, is only protected under special circumstances.

Confidentiality

All reporting channels must maintain the identity of the whistleblower confidential. The identity of persons who are the subject of the report and of other persons named in the report is also confidential. Whistleblowers who provide false information through gross negligence or wilful misconduct are not protected. Only under special circumstances may the reporting channel forward the identity of the whistleblower to the competent authority, for example in the context of criminal proceedings. If the whistleblower consents, his identity may also be disclosed if the disclosure is necessary for follow-up measures. In contrast, no consent is required for the disclosure of the identity of persons affected by the whistleblowing, insofar as this is necessary for follow-up measures or internal investigations, among other things.

Internal reporting channels

Affected companies and institutions

Employers with 50 or more employees are obliged to set up an internal reporting channel. The minimum number of employees does not apply to employers in certain risk sectors, such as capital management companies.

Forms of organisation for internal channels

Companies can set up an internal reporting channel by assigning an employee or a work unit with the task. Alternatively, Section 14 HinSchG allows a "third party" to be entrusted with it. A third party within the meaning of Section 14 also includes a reporting channel that is set up at another group company and is to take over tasks for several independent group companies. The responsibility for reviewing and remedying the reported breach remains with the commissioned company. Several employers with fewer than 250 employees may set up a joint reporting channel.

Requirements for internal channels

Employers can set up oral or written reporting channels. A number of things must be taken into account here: Reporting channels must be designed in such a way that only the persons responsible for receiving and processing the reports have access to the incoming reports. This cannot be guaranteed by setting up a simple e-mail address or internal telephone number. Basically, two options remain: setting up an external telephone number with number suppression or an IT-based system. An IT-based system is likely to be more

cost-effective than having the internal or external person in charge always available by phone.

The responsible persons perform their duties independently and must have the necessary expertise. For small and medium-sized companies in particular, the question arises whether it is worthwhile to set up their own reporting system, to assign internal staff to process reported breaches and to qualify them for this - or whether it is more efficient to assign an experienced ombudsperson, such as a lawyer, to receive and initially process the reports. The concern that hotlines will be flooded with poorly substantiated reports is rather unjustified. Data from the USA shows that a company with 1,000 employees can expect an average of five reports per year.
It should be noted that the establishment and use of internal reporting channels also requires a data protection impact assessment (DPA) in individual cases.

Procedure for internal reporting channels

According to Section 17 HinSchG, the internal reporting channel must:

- Acknowledge receipt of the report to the whistleblower within seven days;
- Check whether the reported breach falls within the material scope of the HinSchG;
- Check the validity of the report;
- Ask the whistleblower for further information if necessary;
- Take appropriate follow-up action;
- Provide feedback to the whistleblower at the latest after three months regarding the follow-up measures planned and taken, as long as this does not affect investigations or the rights of data subjects;
- The information must be documented in compliance with the confidentiality requirement and stored for three years after the conclusion of the procedure.

Dealing with anonymous reports

The handling of anonymous reports was very controversial during the legislative process, which led to unclear regulations. Internal reporting channels are not legally obliged to accept anonymous reports. However, they "should" process them. The corresponding ISO standards (ISO 37301, ISO 37001) nevertheless require the acceptance of anonymous reports. Companies seeking certification must therefore accept and process anonymous reports.

Disclosure

Disclosure refers to making information about breaches available to the public. This includes not only classic notifications to the press, but also postings in social media under certain circumstances.

Disclosure is protected under Section 32 only if:

- An external reporting channel informs the company, and the company does not take any action within the time limits for a response, or the whistleblower does not receive any feedback on taking such follow-up action, or
- In an emergency, or if there is a risk of reprisals even in the case of an external report, if evidence could be suppressed or destroyed, or other circumstances exist that cast doubt on the effective intervention of an external reporting channel.

If the reporting channel does not pass on the information to the company in time and the employee turns to the public for this reason, this can trigger a claim for damages by the company against the reporting channel. Disclosure of incorrect information is prohibited.

Rules of procedure

A whistleblower cannot be held legally responsible for obtaining and accessing information that he has reported or disclosed, as long as the obtaining and accessing does not in itself constitute an independent criminal offence. Whistleblowers are protected from

reprisals and retaliation. This is now subject to a reversal of the burden of proof: if a whistleblower alleges such discrimination, the employer must prove that it is not related to the report.

Compensation and fines

The HinSchG contains two new provisions on damages. Firstly, the whistleblower must be compensated for the resulting damage in the event of a breach of the prohibition of reprisals. However, the employer is not obliged to continue to employ the whistleblower. Secondly, the whistleblower must compensate the damage caused by a deliberate or grossly negligent false report or disclosure. Companies that do not set up a reporting channel, obstruct reports or use reprisals will face fines of up to 50,000 euros from 1 December 2023. However, fines of up to 20,000 euros are also foreseen for persons who knowingly disclose incorrect information.

Entry into force

For employers with more than 250 employees, the obligations of the HinSchG will already apply from 2 July 2023, for smaller companies only from 17 December 2023. The provisions on fines will come into force on 1 December 2023. If employers with more than 50 employees have not yet set up an internal reporting channel, they should do so immediately. When planning the timing, it should also be borne in mind that such a procedure is normally subject to co-determination in the countries, like Germany, that provide for such a mechanism.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Alisha Daley-Stehr Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

Alliuris in Germany

Firm	Herfurth & Partner Luisentraße 5, D-30159 Hanover
Web	www.herfurth.de
Fon	+ 49 511 30756 0
Fax	+ 49 511 30756 10
Mob	
Contact	Ulrich Herfurth, Partner
Language	German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish
Mail	info@herfurth.de

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt