Whistleblowing system: professionally organising whistleblowing in industrial companies

A whistleblowing system is an organised reporting procedure through which employees, suppliers and third parties can report compliance violations within the company. For industrial companies and suppliers it has become particularly relevant since the Whistleblower Protection Act (HinSchG), which obliges certain companies to set up an internal reporting channel. In procurement, it directly affects issues such as supplier compliance, corruption prevention and an intact supply chain.

As of October 2026 · amplifa-marketplace.ai/en/glossary/hinweisgebersystem

Key facts at a glance

01 A whistleblowing system allows internal and external reports on concrete or suspected violations of laws and internal rules.

02 The Whistleblower Protection Act obliges companies with typically 50 or more employees to set up internal reporting channels; the reporting office must operate confidentially.

03 Reports may also relate to misconduct in the supply chain, such as corruption, fraud or violations of codes of conduct.

04 In practice, channels such as email, telephone hotline, online forms or specialised reporting software are frequently combined.

05 Proper handling of the system reduces liability exposure, strengthens the compliance culture and is increasingly also an evaluation criterion in supplier selection.

06 Confidentiality and protection from retaliation are required by law and must be safeguarded organisationally.

Definition: whistleblowing system

A whistleblowing system denotes the entirety of reporting channels, organisational responsibilities and procedures through which reports of violations are received, investigated and followed up. It covers both the technical infrastructure and the personnel and procedural arrangements.

Legal framework at a glance

The legal basis in Germany is the Whistleblower Protection Act (HinSchG), which implements the EU Whistleblower Directive. Under this law, companies with typically 50 or more employees must set up at least one internal reporting channel that allows confidential communication with the reporting person. Company-specific requirements and the appropriateness of the design should always be reviewed on a case-by-case basis.

- Obligation to provide internal reporting channels with typically 50 or more employees
- Requirements for confidentiality and a non-disclosure period for reporting persons
- Protection from retaliation and the prohibition of disadvantage
- External reporting offices of the federal government and federal states as a second instance

Distinction from compliance hotline and ombuds office

The terms are often used synonymously, but there are differences. A compliance hotline is usually only a single channel, whereas the whistleblowing system encompasses the entire process from reporting through investigation to documentation and feedback. An ombuds office is an external person or law firm that acts as a neutral channel and decouples the reporting person from the organisation.

Relevance for purchasing and procurement

Procurement is one of the functions most vulnerable to corruption: purchasing volumes, personal contacts with suppliers and discretion in supplier selection create incentives for bribery, bundling of orders or data misuse. A functioning whistleblowing system is therefore a central control instrument.

Typical report scenarios in the procurement context

Reports can relate to internal violations, but also to misconduct by suppliers or service providers. In practice, issues such as kickbacks, price infiltration, failure to meet quality standards for loaned goods or manipulation of delivery notes are accumulating. Violations of supply chain due diligence obligations, such as human rights or environmental violations at sub-suppliers, also fall within scope.

- Favouring individual bidders in the award process
- False labelling or declaration of origin of goods
- Violations of codes of conduct in the supply chain
- Misuse of confidential tender data or calculations

Link with supplier management and pre-qualification

The whistleblowing system draws on data that also arises in supplier management. Findings from reports flow into the evaluation of suppliers and can alter the evaluation criteria in future tenders. Conversely, suppliers should be informed of the existence of the whistleblowing system as part of the pre-qualification process, so that external reports can also flow in.

Methods and approach for setting up the system

An effective whistleblowing system is created in several steps: define organisation and responsibilities, define channels, create procedural documentation and train the organisation. A structured measures pipeline helps to systematically work through all statutory and internal requirements.

Select reporting channels

Typical channels are an online reporting portal, an anonymous telephone hotline, a dedicated email address or a personal conversation with the reporting office. Combining several channels increases accessibility. An external channel such as an ombuds office or a service provider can increase acceptance where there is fear of retaliation.

Define procedure and case handling

The core is a documented procedure: confirmation of receipt of the report, review of jurisdiction, non-disclosure period for follow-up questions to the reporting person, deadlines for feedback (statutorily typically three months for feedback to the reporting person), internal case management and escalation paths. In deliberately pending cases, such as an investigation of suppliers, it is advisable to involve a defined emergency procurement team configuration in order to adjust procurement activities at short notice.

- Confirmation of the report within the statutory deadline
- Discretion: involve only the persons necessary for the review who need to be involved
- Documentation of the review steps and results
- Obligation to provide feedback to the reporting person

Awareness raising and training

A system only works if it is known and accepted. Training for buyers and managers, intranet pages and brief notes in the onboarding pack increase visibility. Communication to suppliers is also important, for example via the supplier code of conduct or standardised NDA requirements, so that external parties know the reporting channels.

Key KPIs and quality characteristics

Although whistleblowing systems, with quality characteristics such as confidentiality and data protection, can hardly be reduced to a single figure, there are practicable key figures with which

effectiveness can be measured. The goal is not to maximise the number of reports, but a healthy reporting system in which errors become visible and are addressed.

Report volume and channel distribution

A sudden sharp decline in the number of reports can be just as much a warning signal as an abnormal increase, which may point to communicated maldevelopments or conflicts. The distribution across channels shows which routes are actually used by employees and helps to further develop the system.

Processing quality and deadlines

Key metrics include adherence to confirmation and feedback deadlines, the proportion of substantiated reports, the duration of case handling and the proportion of conclusively documented cases. Companies with established reporting processes present these data in overviews that are expected by auditors and customer enquiries in the context of supplier evaluation.

Risks, controls and data protection

The main failures of whistleblowing systems are lack of confidentiality, insufficient independence of the reporting office and incomplete documentation. Added to this are data protection requirements, which must be strictly observed when storing and sharing personal data. These points should be reviewed regularly; for legal assessment in individual cases, expert advice is recommended.

Confidentiality, anonymity and data protection

Confidentiality means that only the reporting office knows the identity of the reporting person, unless they expressly consent. Anonymous reports are permitted, but make follow-up questions more difficult. Reports are stored on the basis of data governance with defined access rights and deletion periods; the data protection officer should be involved in the design.

Misuse and deliberately false reports

Not every report is well founded. The system must be designed so that deliberately false reports can be traced and, if necessary, addressed under employment law, without deterring legitimate reporting persons. Clear internal rules for handling reports in good faith and an accessible contact person reduce potential for conflict.

Integrating controls in procurement

Reports from the procurement environment should flow into existing control mechanisms: the four-eyes principle for release of purchase orders, regular market analyses to validate prices, and documented multiple offers (multiple sourcing) have a preventive effect. If a supplier is flagged by a report, a targeted request for documents or an enhanced audit regime (carrier performance or supplier evaluation) may follow.

Current developments and outlook

Regulatory pressure is increasing: alongside the Whistleblower Protection Act, requirements from supply chain due diligence, sustainability reporting and customer requirements in the context of supplier audits are taking effect. Whistleblowing systems are thus evolving from a pure compliance instrument to a building block of the ESG and resilience agenda.

Integration with supply chain due diligence and sustainability

Reports on working conditions, environmental obligations or raw material origins at sub-suppliers are increasingly becoming part of due diligence processes. Companies integrate whistleblowing systems into risk maps and remedial measures and also establish reporting channels via supplier portals and the supplier code of conduct.

Digitalisation and AI-supported case support

Modern systems offer automated confirmation of receipt, encryption, translation and structured categorisation of reports. In practice, analyses for the early detection of patterns are also becoming established, for example conspicuous patterns in awards or prices. It remains important that automation supports confidential case handling by humans rather than replacing it.

Typical metrics

Metric	Typical value
Confirmation deadline met	100 % within 7 days *statutory deadline; document any deviations*
Feedback rate to reporting persons	> 95 % *proportion of substantiated cases with feedback provided on time*
Proportion of substantiated reports	typically 20–50 % *healthy signal range; very low values indicate communication deficits*
Average case processing time	30–90 days *heavily dependent on case complexity; the shorter, the more credible the system*

Practical example

A mid-sized mechanical engineering company with around 120 employees and a highly fragmented supplier portfolio introduces a structured whistleblowing system following a customer enquiry in the context of a supplier audit. Several reports reach the system indicating excessively close contacts between a buyer and a particular mechanical components supplier. The review reveals inflated prices and undocumented side agreements. The case leads to a re-tender with multiple sourcing, a tightening

of the evaluation criteria and an extension of the supplier code of conduct, which is communicated to all suppliers via the pre-qualification process.

- Introduction of an anonymous online reporting portal in addition to an internal email address
- Definition of a documented case procedure with clear responsibility within the compliance function
- Linking the analysis of reports with supplier evaluation and pre-qualification
- Training of all buyers and informing suppliers via the supplier code of conduct

Conclusion

For industrial companies, a whistleblowing system has long been more than a statutory obligation: it is an early warning system that makes risks within the company and the supply chain visible. For buyers, it provides direct insights into corruption and quality risks and strengthens their position vis-à-vis suppliers and customers. What matters is not mere set-up, but consistent embedding in processes, training and supplier communication. Those who take confidentiality, data protection and processing quality seriously gain trust on all sides. In this way, the whistleblowing system becomes a supporting pillar of modern supplier management.

Frequently asked questions

? From what point are companies required to set up a whistleblowing system?

Under the Whistleblower Protection Act (HinSchG), companies with typically 50 or more employees must set up at least one internal reporting channel. Smaller companies are generally not subject to this obligation, provided no special requirements arise from other regulations. The exact design should be reviewed on a case-by-case basis.

? Must a whistleblowing system allow anonymous reports?

Anonymous reports are not strictly required by law, but are considered best practice because they lower the barrier for reporting persons. Confidentiality, by contrast, is mandatory: the identity of the reporting person must not be disclosed without their consent. Many companies therefore deploy systems that technically enable anonymous reporting.

? What deadlines apply to the handling of reports?

As a rule, receipt of a report must be confirmed within seven days. The reporting person receives feedback typically within three months and at the latest four weeks after completion of the procedure. Missed deadlines should be documented and justified.

? Can suppliers or external persons also submit reports?

Yes, the Whistleblower Protection Act also protects external reporting persons such as suppliers, customers and consultants. Many companies therefore publicise their system via the supplier code of conduct, the supplier portal or the pre-qualification process. External reports on supplier misconduct are particularly valuable for procurement.

? What happens to false or malicious reports?

Deliberately false reports are not protected under the Whistleblower Protection Act and can have consequences under employment or criminal law. It is important that the procedure documents the assessment of the substance of a report, so that well-founded and unfounded reports can be distinguished. Fair treatment protects reporting persons without legitimising abusive reports.

? What does a whistleblowing system cost for a mid-sized company?

The costs depend on the chosen approach: a simple internal reporting channel via email and telephone is virtually free in practice, but requires personnel capacity. External ombuds offices or dedicated reporting portals generate ongoing costs, typically in the low to mid four-figure annual range. The robustness of internal case management matters more than the system costs.

Find the right suppliers on Amplifa

Verified industrial suppliers in Germany, Austria and Switzerland. Describe your requirement and receive comparable offers.

amplifa-marketplace.ai