GUIDE 2025/2026

Whistleblowing guide for mid-sized companies

The German Whistleblower Protection Act, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is the HinSchG? 3

1.1 The act in plain words 3

1.2 Scope — what gets reported? 3

1.3 Protecting whistleblowers 3

1.4 Internal vs. external reporting channels 4

2 Who needs a reporting channel? 5

3 The road to compliance — seven phases 7

4 What does implementation cost? 9

5 The ten most common mistakes 11

6 Readiness check: are you ready? 13

7 Glossary 15

8 Your next step 17

1 What is the HinSchG?

1.1 The act in plain words

The **German Whistleblower Protection Act (HinSchG)** transposes the EU Whistleblowing Directive (2019/1937) into German law. Since **2 July 2023** it has obliged companies and organisations to set up secure channels for reporting breaches of the law, and to protect whistleblowers from retaliation.

Unlike other compliance subjects, this one is not about IT security or data protection. It is about **company culture**, obeying the law, and protecting the people who bring wrongdoing to light. In practice: every member of staff — and certain outsiders — has to know of a reporting channel they can clearly reach.

> **The core idea:** the act does not ask "is anything wrong in your company?" but "can your people report safely and in confidence if something is — and do they know how?"

The sanctions are moderate but real: failing to set up a channel risks a fine of up to **50,000 euros**. Obstructing a report, or retaliating against a whistleblower, up to **100,000 euros**. On top of that comes liability in damages towards the whistleblower.

1.2 Scope — what gets reported?

The act protects reports of:

- **Criminal offences** under German law
- **Regulatory offences carrying a fine**, where the rule protects life, health, the rights of employees or their representative bodies
- **Breaches of EU law** in ten fields, among them public procurement, financial services, product safety, transport, environmental protection, consumer protection, data protection and food safety
- **Breaches of the rules** against money laundering, terrorist financing and tax evasion

Outside the scope: personal disputes, individual employment questions that involve no breach of law, and political opinions.

1.3 Protecting whistleblowers

Anyone making a report under the act is protected by law against:

- Dismissal, or a contract not being renewed

- A formal warning, transfer or demotion
- Discrimination, bullying or intimidation
- A negative appraisal or reference
- Being refused training or promotion
- Any other detrimental treatment

> **The burden of proof is reversed:** in a dispute the company has to prove that a measure — a dismissal, say — was *not* connected to the report. That raises the liability risk considerably.

1.4 Internal vs. external reporting channels

The act recognises two kinds of reporting channel:

Type	Who?	Mandatory?
Internal channel	Set up by the company itself	Mandatory from 50 employees
External channel	The Federal Office of Justice (BfJ), state police offices and others	Always available to whistleblowers

Whistleblowers may choose between the internal and the external route — they are not obliged to go internally first. An attractive internal system therefore reduces the likelihood of reports going outside, to authorities or to the press.

> **Worth knowing:** the internal channel can be run by someone outside the company — a law firm, or an external provider such as iso-easy. That frees internal resources and secures independence.

2 Who needs a reporting channel?

The basic rule: from 50 employees

The duty to run an internal channel applies to every company with **50 or more employees**. Below that threshold there is no legal duty — but smaller companies can set one up voluntarily to reduce their compliance risk.

50+ staff	7 days	3 months
a channel becomes mandatory	to acknowledge receipt	to report back to the whistleblower

Special thresholds and special rules

- **From 50 staff, phased in:** the deadline was 17 December 2023, and the duty has applied since then with no transition period.
- **The financial sector:** banks, investment firms and insurers have to run a channel **whatever their size** .
- **Groups:** the parent can centralise the channel — with the subsidiaries' agreement and clear responsibilities.
- **A shared channel:** companies with up to 249 staff may share a channel with others, and save on cost.

Who can report?

- Your own staff, interns and agency workers included
- Managing directors and board members
- Self-employed providers and freelancers
- Job applicants and former staff
- Suppliers and contractual partners
- Shareholders and supervisory board members

What the internal channel has to do

- **to acknowledge receipt** within **7 days**
- **Independent examination** of the report
- **Feedback** to the whistleblower within **3 months** (on the measures taken)
- **Documentation** of every report, in a way that satisfies data protection law

- **Confidentiality** of the whistleblower's identity
- **Reachable by more than one route**: in writing, orally, and face to face on request

> *A real example: a machine builder with 85 staff has ignored the act. A former employee reports environmental breaches straight to the public prosecutor. The investigation uncovers the missing channel — a fine of €30,000, plus the damage to reputation.*

Anonymous reports

Since the 2023 amendment, internal channels have to process anonymous reports as well. That raises acceptance and willingness to report considerably. Software-based systems with anonymous communication are the current standard.

3 The road to compliance — seven phases

Setting this up is one of the simpler pieces of compliance. Depending on your size, implementation takes only **two to six weeks**.

1. **Scoping and legal analysis**

   Check whether the act applies: headcount, industry (financial sector?), group structure. Decide whether to run your own channel or share one. One week.

2. **Decide: run it internally or not**

   Should your own people run it — compliance, HR, legal — or an external provider, a law firm or a specialist? Weigh cost against independence and expertise. One week.

3. **Set up the technical system**

   Choose the software: a web portal, anonymous communication, several languages. The alternative is a simple mailbox with clearly defined access rights. The requirement either way: anonymity has to be assured. One to two weeks.

4. **Write the procedure**

   An internal policy: how are reports handled, who is responsible, how do you communicate, what are the deadlines, what escalation steps exist? One week.

5. **Inform your staff**

   This is mandatory: everyone is actively told about the channel — intranet, notice, e-mail, the induction pack — and their acknowledgement is recorded. In several languages for international teams. One week.

6. **Train the managers**

   Managers need to know what happens when a member of staff comes to them as a whistleblower, which actions are prohibited, and what support they have to give. Record the training. One week.

7. **Running it, and annual reporting**

   The channel handles incoming reports to the agreed deadlines: seven days to acknowledge, three months to report back. An annual report to management with anonymised figures. Ongoing.

> **Tip:** Start with a software-based system that allows anonymous reports. It costs barely more than a mailbox (from €99 a month), and the gain in data security and legal certainty is considerable.

4 What does implementation cost?

This is one of the cheapest compliance requirements there is — if you go about it the right way. Typical ranges:

Company size	One-off build*	Monthly cost	Timeframe
50–99 staff	**€1,490–1,990**	**€99/month** (external channel)	2–4 weeks
100–249 staff	**€1,990–2,990**	**€99–149/month**	3–6 weeks
250–499 staff	**€2,990–4,990**	**€149–249/month**	4–8 weeks
500–2,499 staff	**€4,990–8,990**	**€249–499/month**	6–12 weeks
2,500+ staff	**€8,990–14,990**	**€499–999/month**	8–14 weeks

* Includes legal advice, the policies, setting up the software, training managers and informing staff. **Excludes** handling the reports themselves.

What drives the cost?

- **How many sites you have:** each may need its own languages and its own manager training.
- **How many languages:** the portal often has to be available in English, Turkish, Polish and Romanian.
- **Your industry:** the financial sector has additional requirements towards BaFin.
- **Integration:** connecting it to an existing compliance management system.

The external channel as a model

For a mid-sized company the most cost-effective option is a **fully external channel**. The advantages:

- Independence and confidentiality are assured
- Legal judgement from experienced specialists
- No load on your own resources
- Reachable round the clock through the platform
- A fixed monthly price instead of variable staff costs

In the interest of transparency: many providers charge €300–800 a month for an external channel. Our entry price from €99 a month is possible through software automation, at the same level of legal certainty. Complex cases are billed additionally at an hourly rate from €190, transparently.

5 The ten most common mistakes

From setting up a good many of these channels, we know the usual stumbling blocks:

1. **“We do not have problems” — and so no channel at all**
   A false assumption: the duty applies whether or not anything is actually wrong. No channel means a direct risk of a fine.

2. **Refusing anonymous reports**
   Since the 2023 amendment, anonymous reports have to be processed. A channel that refuses them does not comply.

3. **A channel that is not independent**
   The person responsible sits in a hierarchical conflict — the direct manager of some of the staff, for instance. That cuts both willingness to report and trust.

4. **Only one language**
   With international teams the channel has to be reachable in the relevant languages — otherwise access is not free of discrimination.

5. **Communicating it poorly**
   The channel exists but nobody knows about it. Making it known is a duty — and the evidence, intranet screenshots or mailing lists, has to exist.

6. **Missing the deadlines**
   Seven days to acknowledge, three months to report back. Missing them breaches your duties — and gives the whistleblower reason to go outside.

7. **No training for managers**
   Managers have to know that they may not disadvantage a whistleblower. Without training, retaliation can happen unintentionally — and with personal liability.

8. **An insecure route (unencrypted e-mail)**
   Unencrypted e-mail is not a compliant channel. The whistleblower's identity could become accessible to others.

9 **No documentation**

Every report has to be documented, with the identity protected. Without it you can prove nothing later — including in litigation.

10 **Failing to prevent retaliation**

The burden of proof is reversed: if a whistleblower suffers a disadvantage after reporting — a worse appraisal, say — the company has to prove there is no connection. That is hard without clear processes.

6 Readiness check: are you ready?

Answer the following ten questions honestly, yes or no:

1. **Do you have 50 or more employees, counting the group where relevant?**
   The threshold at which the channel becomes mandatory.
2. **Do you have an internal reporting channel?**
   Run in house or outsourced to an external provider.
3. **Can the channel take anonymous reports?**
   Mandatory since the 2023 amendment.
4. **Have all staff been demonstrably informed?**
   Intranet, notice, e-mail, induction material.
5. **Have managers been trained on the act?**
   Above all on the ban on retaliation and the duty of confidentiality.
6. **Do you have a documented case-handling procedure?**
   Seven days to acknowledge, three months to report back, an escalation matrix.
7. **Is the channel reachable in every relevant language?**
   For international teams, English, Turkish, Polish and Romanian are often needed.
8. **Is the confidentiality of the whistleblower's identity assured technically?**
   Encryption, access control, anonymous communication.
9. **Is there an annual report to management?**
   Anonymised figures, with no personal detail.
10. **Does the channel sit independently of day-to-day operations?**
    With no direct line of authority over the people who might be concerned.

Your yes answers	Assessment	Recommendation
0–3 × yes	**Acutely exposed**	If the act applies to you, set the channel up now. Two to four weeks.

Your yes answers	Assessment	Recommendation
4–6 × yes	**Partly prepared**	Focus on the gaps, usually training and documentation. Two to three weeks.
7–10 × yes	**A good basis**	Fine-tuning and an annual review. Day-to-day operation is running.

7 Glossary

HinSchG

The German Whistleblower Protection Act — in force since 2 July 2023, transposing the EU Whistleblowing Directive.

EU Whistleblowing Directive

Directive (EU) 2019/1937 — the EU framework protecting whistleblowers.

Whistleblower

Someone who reports a breach of the law, internally or externally.

Reporting channel (internal)

The office set up by the company to receive reports. Mandatory from 50 employees.

Reporting channel (external)

An official body — the Federal Office of Justice, state police offices and others — that takes reports independently of the company.

BfJ

The Federal Office of Justice — the central external reporting channel at federal level.

Retaliation

Any measure that disadvantages a whistleblower because of their report. Prohibited.

Reversed burden of proof

In a dispute the company has to prove that a measure had nothing to do with the report.

Duty of confidentiality

The whistleblower's identity may be disclosed only to a narrowly defined group of people.

Anonymous report

A report without a name. Since the 2023 amendment it has to be processed.

Case management

Handling incoming reports in a structured way, with deadlines, documentation and an escalation matrix.

Shared channel

A channel run jointly by several companies, each with up to 249 staff.

Scope

The subjects the act covers, defined by law: criminal offences, breaches of EU law and others.

Fine

Up to €50,000 for having no channel, up to €100,000 for retaliation or for obstructing reports.

8 Your next step

You have read this guide — that is the first step already. Complying with the act takes manageable effort and protects you from fines, from damage to your reputation and from personal liability at management level.

A free first conversation

In 30 minutes, with no obligation, we work out together:

✓ Does the act apply to you?

✓ What would a legally sound reporting channel look like?

✓ What will it cost you?

✓ What are the next steps?

No sales pitch, no pressure — just an honest assessment.

The quick whistleblowing check

At **iso-easy.de** you will find our free whistleblowing check. In a few minutes you get a view of what applies to you and what it takes.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and compliance we support mid-sized companies in implementing whistleblower protection, the GDPR and neighbouring subjects — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.