

Klosterfrau Group

Information on the Whistleblower Protection Act („Hinweisgeberschutzgesetz“) and the “Hintbox” Whistleblowing system

Contents

1.	What does the Whistleblower Protection Act (Hinweisgeberschutzgesetz (HinSchG)) mean for our corporate group?.....	2
2.	What reporting channels are available?.....	2
3.	Will my identity as a whistleblower remain protected? Is anonymous reporting possible?	3
4.	Are all persons who report incidents covered by whistleblower protection?	3
5.	What is the whistleblowing system intended for - and what is it not intended for?.....	4
6.	Who receives the internal report?	4
7.	What procedure is followed when an internal report is submitted?	5
8.	How can you access our internal whistleblowing system?	5
9.	Data protection aspects	5

1. What does the Whistleblower Protection Act (Hinweisgeberschutzgesetz (HinSchG)) mean for our corporate group?

The HinSchG requires companies to establish secure channels for reporting misconduct. For us, however, it means more than simply fulfilling a legal obligation: it is a central component of our compliance management system and provides the framework to further strengthen an open and safe feedback culture. We create a protected space for issues that might otherwise go unheard.

A large part of our compliance measures is aimed at preventing violations from occurring in the first place. By continuously improving prevention, we aim to actively protect our employees and the entire company from future harm.

In addition to our routine audits, we also rely on a culture of attentiveness. If irregularities should occur despite all precautions, our whistleblowing system offers our employees or external partners (such as customers or suppliers) the opportunity to alert us.

We have chosen the digital whistleblowing system "Hintbox". It provides you with an absolutely confidential way to submit concerns securely.

2. What reporting channels are available?

If you observe an irregularity, you can choose between internal and external state reporting channels. We encourage you to use our internal channel first, as this allows us to respond directly and most quickly. However, if an internally reported violation is not resolved, you are of course free to contact an external authority.

a) Our internal whistleblowing system: Who can use it?

Our Hintbox, as the internal reporting office of the Klosterfrau Group, is available as a secure channel to our own employees as well as our business partners, suppliers, and third parties.

b) State (external) reporting offices

In addition to our system, the legislator has established official contact points at the federal level. These are:

- Federal Office of Justice (BfJ): The central federal reporting office, accessible via the BfJ website. It operates completely independently from the rest of the BfJ's areas of responsibility.
- Federal Financial Supervisory Authority (BaFin): Responsible for reports in the area of financial services.
- Federal Cartel Office (BKartA): The contact point for reports related to competition violations.

c) How can a report be submitted?

You can submit your report in various ways:

- **In writing or verbally:** Reports can be submitted in text form or via voice transmission (e.g., telephone).
- **Anonymously:** Through Hintbox, you can submit information without revealing your identity.
- **Secure dialogue:** Even with an anonymous report, we remain in contact with you. Through a protected login with a password, you can answer follow-up questions or check the processing status without compromising your anonymity.

3. Will my identity as a whistleblower remain protected? Is anonymous reporting possible?

Protecting your identity and ensuring the confidentiality of information are at the core of our reporting procedure.

- **Confidential processing:** Only the individuals responsible for receiving and handling reports, as well as the specialists supporting them, have access to incoming reports. We treat your identity and the names of other persons mentioned in the report with strict confidentiality, if you wish.
- **Anonymous communication:** Reports can also be submitted completely anonymously. Through our "Hintbox," communication with you is still possible - for example, to clarify follow-up questions - without compromising your anonymity.
- **When protection ends:** Your identity is generally protected. Disclosure only occurs in legally prescribed exceptional cases. It is important to know: this protection does not apply in cases of deliberately false information. Anyone who intentionally or through gross negligence spreads untruths must expect that their identity may be disclosed - for example, to allow affected persons to defend themselves legally.

4. Are all persons who report incidents covered by whistleblower protection?

Protection for whistleblowers applies under certain conditions:

- **Requirement for protection:** You are protected if, at the time of reporting, you had sufficient reason to believe that the information was true and could indicate a violation.

- **Protection against discrimination:** Protected individuals must not face any professional disadvantages as a result of their report. This means that no negative legal or employment-related consequences - such as termination or formal warnings - may occur because of a whistleblowing report.

5. What is the whistleblowing system intended for - and what is it not intended for?

The Hintbox is an important tool for protecting the integrity of our company. To ensure it serves its purpose, please observe the following guidelines:

- **Purpose of reporting:** Only reports concerning violations of applicable law (EU, federal, or state law) or internal company regulations should be submitted via Hintbox. The system is intended to uncover misconduct and is explicitly *not* meant for denunciation.
- **Truthfulness:** Please only submit reports for which you can reasonably assume that the described facts are true. If you are unsure whether certain information is correct or if it is based on assumptions or statements from third parties, please explicitly indicate this in your report.
- **Risks of false reports:** Deliberately false allegations must be strictly avoided. Anyone who intentionally or through gross negligence submits false information not only loses their protection status but must also expect legal consequences. These may include claims for damages by affected individuals or fines of up to 20,000 euros imposed by authorities.

6. Who receives the internal report?

As soon as you submit a report via Hintbox, it is forwarded directly to the responsible internal reporting office.

- **Composition of the reporting office:** The reporting offices of each company within the corporate group consist of the Chief Compliance Officer (CCO), a representative from the HR department, and - where applicable - the chairperson of the works council.
- **Strict separation and confidentiality:** Technical safeguards ensure that each reporting office only has access to the reports belonging to its respective company. In addition, all involved persons are bound to the highest level of confidentiality. This guarantees that your anonymity - if requested - remains protected and that your data is treated with absolute confidentiality in every case.

7. What procedure is followed when an internal report is submitted?

As soon as you submit a report, a clearly defined process begins to ensure transparency and security:

- **Acknowledgment of receipt:** Within 7 days of receiving your report, the internal reporting office will send you a confirmation that your report has been received.
- **Processing and communication:** The reporting office carefully examines the matter. If necessary - and if you wish - the internal reporting office will communicate with you via Hintbox to clarify any open questions.
- **Assessment of follow-up measures:** Depending on the outcome of the review, appropriate steps will be taken. These may include internal investigations, discontinuation of the procedure (if the suspicion is not confirmed), or forwarding the case to a competent authority, such as the public prosecutor's office in the event of criminal offenses.
- **Feedback:** No later than 90 days after your report, you will receive an update on the current status and the planned or already implemented measures. For legal reasons, no confidential details (such as the initiation of a specific criminal proceeding) will be disclosed; instead, you will be informed in general terms about the next steps.

8. How can you access our internal whistleblowing system?

We offer you several ways to securely and easily submit your report:

- **Online via Hintbox:** By using the link <https://klosterfrau.interne-meldestelle.de> you can access the homepage of our digital reporting system directly. There, you will be guided step by step through the process.
- **Report via company account:** You also have the option to submit a report through the account klosterfrau@interne-meldestelle.de. Your report will be transmitted directly into our reporting system via a secure interface. Confidential processing by the responsible offices is ensured at all times.
- **Telephone reporting:** Alternatively, you can contact us by phone at **+49 800-0002461**. During the call, you will be asked specific questions about the matter. Your answers will then be carefully entered into our internal reporting system and processed further.

9. Data protection aspects

When receiving and processing reports, personal data is processed - such as the names of

whistleblowers (unless they submitted their report anonymously), accused persons, or witnesses, as well as details that allow conclusions to be drawn about individuals. Our reporting channels are established and operated pursuant to the requirements of the General Data Protection Regulation (GDPR). In particular, your data is used exclusively for the purpose of clarifying the reported issue and is protected against unauthorized access through technical and organizational measures.

For more information, please see the Privacy Notice for the Klosterfrau Group's Whistleblowing system (<https://klosterfrau.interne-meldestelle.de/privacy-system>).

Cologne, August 2026



Dr. Stefan Koch
CEO



Jesco Thiele
Chief Compliance Officer (CCO)