

---

KARL MAYER Holding SE & Co. KG

---

# RULES OF PROCEDURE FOR THE COMPLAINTS PROCEDURE

---

November 1, 2023

---



## Table of contents

<b>1. Purpose of the Rules of Procedure</b>	<b>3</b>
<b>2. Scope of application</b>	<b>3</b>
<b>3. Complaints channels</b>	<b>3</b>
<b>4. Confidentiality and protection</b>	<b>3</b>
<b>5. Procedural sequence</b>	<b>3</b>
5.1 Receipt of a report	3
5.2 Examination of the report/plausibility check	4
5.3 Clarification of the facts of the matter/examination of the veracity of the incoming report	4
5.4 Devising a solution	4
5.5 Feedback to whistleblower	4
5.6 Annual and ad hoc reporting to the board of management	5
5.7 Adapted preventive concept	5
5.8 Deletion	5

## 1. Purpose of the Rules of Procedure

The absolute observance of laws, ethical principles, and internal guidelines is accorded the highest priority within the KARL MAYER Group. Only if laws and internal ethical and compliance rules are observed can damage to the KARL MAYER Group, its employees, business partners, and other stakeholders be averted at an early stage.

Every form of misconduct within our own business area and the supply chain of the KARL MAYER Group must therefore be identified at an early stage and remedied without delay. This requires alertness and the willingness on the part of all our managers, employees, business partners, and other stakeholders to report possible infringements and misconduct if any concrete indications exist in this regard.

To this end, the KARL MAYER Group has established an in-house whistleblower system through which reports can be filed regarding infringements of laws, rules, and ethics, and risks and infringements in terms of human rights and environmental considerations. These Rules of Procedure regulate the procedure triggered by an incoming report.

The whistleblower system fulfils not only the requirements of the German Whistleblower Protection Act (Hinweisgeberschutzgesetz, HinSchG) but also the requirements regarding the complaints procedure under the German Act on Corporate Due Diligence Obligations in Supply Chains (Lieferkettensorgfaltspflichtengesetz, LkSG). It means that the whistleblower can be certain that they will be comprehensively protected against reprisals if they file a report. Confidentiality and data protection are ensured, of course.

In principle, the whistleblower can choose to use either the aforementioned in-house whistleblower system or contact an external hotline or reporting body (see the detailed information provided on the website of the Federal Office of Justice under "Hinweisgeberstelle" (Whistleblowing Body)). To ensure the report is handled promptly and knowledgeably, the aim should be to encourage whistleblowers to use the in-house whistleblower system.

## 2. Scope of application

The complaints procedure can be used not only by employees and business partners of the KARL MAYER Group but also by external third parties in order to report

- human rights and environmental risks,
- the infringement of human rights and environmental responsibilities, and
- other actual or potential infringements against statutory or in-house regulations

that occur within our business area or within our supply chain.

## 3. Complaints channels

- The Chief Compliance Officer of the KARL MAYER subsidiaries: Ms. Angela Weiland,  
Contact: [Compliance@karlmayer.com](mailto:Compliance@karlmayer.com)
- The ombudspersons of the KARL MAYER subsidiaries: Baker Tilly, Nymphenburger Strasse 3b, 80335 Munich.  
Office hours Mon.–Fri. 8:00 am–6:00 pm  
Contact: +49 89 55066-554 / [Ombudsperson.karlmayer@bakertilly.de](mailto:Ombudsperson.karlmayer@bakertilly.de)
- The complaints system of the KARL MAYER subsidiaries:  
<http://whistle-blowing-system.karlmayergroup.com>

## 4. Confidentiality and protection

Reports will be handled by selected, specially trained employees of the KARL MAYER Group or by the official legal ombudspersons. They are impartial, and in fulfilling their remit they are neutral, not bound by instructions, and they are obliged to respect confidentiality and to uphold the rights of whistleblowers and other affected persons.

Fact-finding measures, consideration and investigation of incoming reports are generally conducted in a **strictly confidential** manner.

The reporting system allows communications to be conducted with the whistleblower via an anonymous mailbox. The system does not save technical data that could permit inferences to be made regarding the whistleblower (IP address, location information, device specifications, etc.). The whistleblower's personal data will only be collected if they choose to share this data. If the whistleblower reveals their own identity, or names another person in their report, this information shall be treated as confidential during the subsequent report handling and follow-up. However, in exceptional cases (such as in the case of criminal offences), the legal obligations of disclosure must be observed towards the authorities.

## 5. Procedural sequence

### 5.1 Receipt of a report

Once a report has been received, its receipt will be documented in the whistleblower system (creation of a digital case file) and assigned internally to a handler. Reports filed via the reporting system are automatically recorded within the system. Reports filed via other channels are manually entered into the system.

Next, the system automatically links three standard processes (Send acknowledgment, Write assessment, and Send report), the completion of which is documented during the course of the procedure within the system.

If a response is possible and provided the whistleblower has not submitted an anonymous report that does not permit a response, they will be notified without delay, but in any case within a period not exceeding **seven days** from the time their report was received.

## 5.2 Examination of the report/plausibility check

The handler examines if the incoming report contains sufficient information for the matter to be investigated.

If there is not sufficient information, the handler will contact the whistleblower and request further information. If the whistleblower does not respond to the attempt to make contact, the case will be closed within a period not exceeding three months from the time the report was received. Next, the whistleblower will be notified of the closure of the case. (For reports filed via the reporting system, this information will be relayed through the "Send report" operation via the anonymous mailbox.)

If sufficient information has been given, the handler uses the "Write assessment" operation to rate the relevance of the matter and write an assessment.

## 5.3 Clarification of the facts of the matter/examination of the veracity of the incoming report

The handler either examines the matter personally or forwards it for examination by the competent entity within the organisation, while respecting the principles of confidentiality and data protection. At this point, the handler assesses the veracity of the report, meaning whether the matter and the whistleblower (reporting person) appear credible, and what consequences the matter could have on the organisation. The anonymity of the report is not a criterion weighing against the veracity of the report.

If necessary, the matter will be discussed with the whistleblower. The following shall be observed in this respect:

- In the case of reports made over the telephone, a permanently retrievable audio recording of the call or a complete and accurate transcript (verbatim record) may only be made with the permission of the whistleblower. Otherwise, it is only permissible to prepare a summary of the contents (substantive record).
- If face-to-face meetings are conducted with the whistleblower, an audio recording of the meeting or a verbatim record may be prepared with the permission of the whistleblower. Alternatively, a substantive record shall be prepared.
- The whistleblower shall be given the opportunity to review the record, to correct it if necessary and confirm it with their signature. If an audio recording is used to prepare a record, this must be deleted as soon as the record is prepared.

In documenting the report, it must be ensured that the documentation is stored at a location accessible to authorised persons only. It is also recommended that substantive records, in particular, be prepared pseudonymously.

In addition, the principle of data economy should also be observed. The handling of personal data by hotlines must, as a rule, be performed in accordance with the applicable regulations. The main regulations are set out in the GDPR and the German Federal Data Protection Act (BDSG) in particular.

Having clarified the facts, and discussed and examined the case, the case will be closed if the handler or the competent entity is of the opinion that no infringement or risk exists as per the scope of application set out in Section 2.

## 5.4 Devising a solution

Having clarified the facts, discussed and examined the case, if the handler or the competent entity is of the opinion that an infringement or risk exists as per the scope of application set out in Section 2, a proposal will be devised regarding the subsequent steps and this must include prevention and remedial measures.

Action must be taken to have legal infringements or abuses promptly eliminated, and to minimise the extent of the damage. If the whistleblower is directly affected, it may be helpful to coordinate the relevant measures with them. The remedial measures should be appropriate, i.e. conducive to ending the infringement conclusively and effectively. If necessary, selected persons from other departments can be integrated into the process at this point. The effectiveness of the measures will be subsequently reviewed at regular intervals, and further steps performed if necessary.

The following possible courses of action should be considered as a minimum requirement:

- investigate for other similar cases existing within the organisation,
- take disciplinary measures against relevant employees,
- issue immediate notifications (for example to data protection authorities in the event of data breaches),
- fulfil any notification and reporting obligations towards shareholders, insurers, authorities, contracting partners etc.,
- tie in the public prosecutor's office by filing a complaint or personally visiting the office,
- claim compensation,
- make reparations to injured parties within the organisation,
- public communication measures in the event of reputational damage.

## 5.5 Feedback to whistleblower

Within three months of acknowledging receipt of the report or, if there was no acknowledgment of receipt, within three months and seven days of receiving the report, the whistleblower must be given feedback detailing the action envisaged or taken as a follow-up to the report, and the grounds for such follow-up based on the legal regulation.

If there has been no infringement (Section 5.3) and the case is closed, the whistleblower shall be informed of the case closure. (For reports filed via the reporting system, this information will be relayed through the "Send report" operation via the anonymous mailbox.) The case file will then be closed.

The case handling time varies depending on the facts of the case, and may therefore take anything from a few days to several months. The KARL MAYER Group endeavours to promptly handle and conclude all reports and subsequent investigations.

## **5.6 Annual and ad hoc reporting to the board of management**

The course of the entire procedure will be documented and filed in accordance with data protection regulations. The procedure and the results shall be summarised in a final report. An ad hoc reports may be issued to the board of management immediately following the conclusion of the procedure. Otherwise, a combined annual report shall be issued to the board of management detailing all reports received and how these were handled.

## **5.7 Adapted preventive concept**

To prevent infringements arising from similar grounds, preventive measures will be implemented, including compliance trainings, revision of the Compliance Guidelines, amendment of the processes and procedural sequence, and planning of review measures.

## **5.8 Deletion**

All reports received by the hotline (reporting body) must be comprehensively documented and securely retained. The documentation must be deleted **three years** after the conclusion of the procedure in accordance with Section 11 (5) of the German Whistleblower Protection Act (HinSchG) or **seven years** after the conclusion of the procedure in accordance with Section 10 (1) of the German Act on Corporate Due Diligence Obligations in Supply Chains (LkSG). However, at this point other retention periods should be considered and fulfilled. The documentation may be retained for a longer period in order to comply with the requirements under this law or other legal regulations, insofar as this is necessary and commensurate.