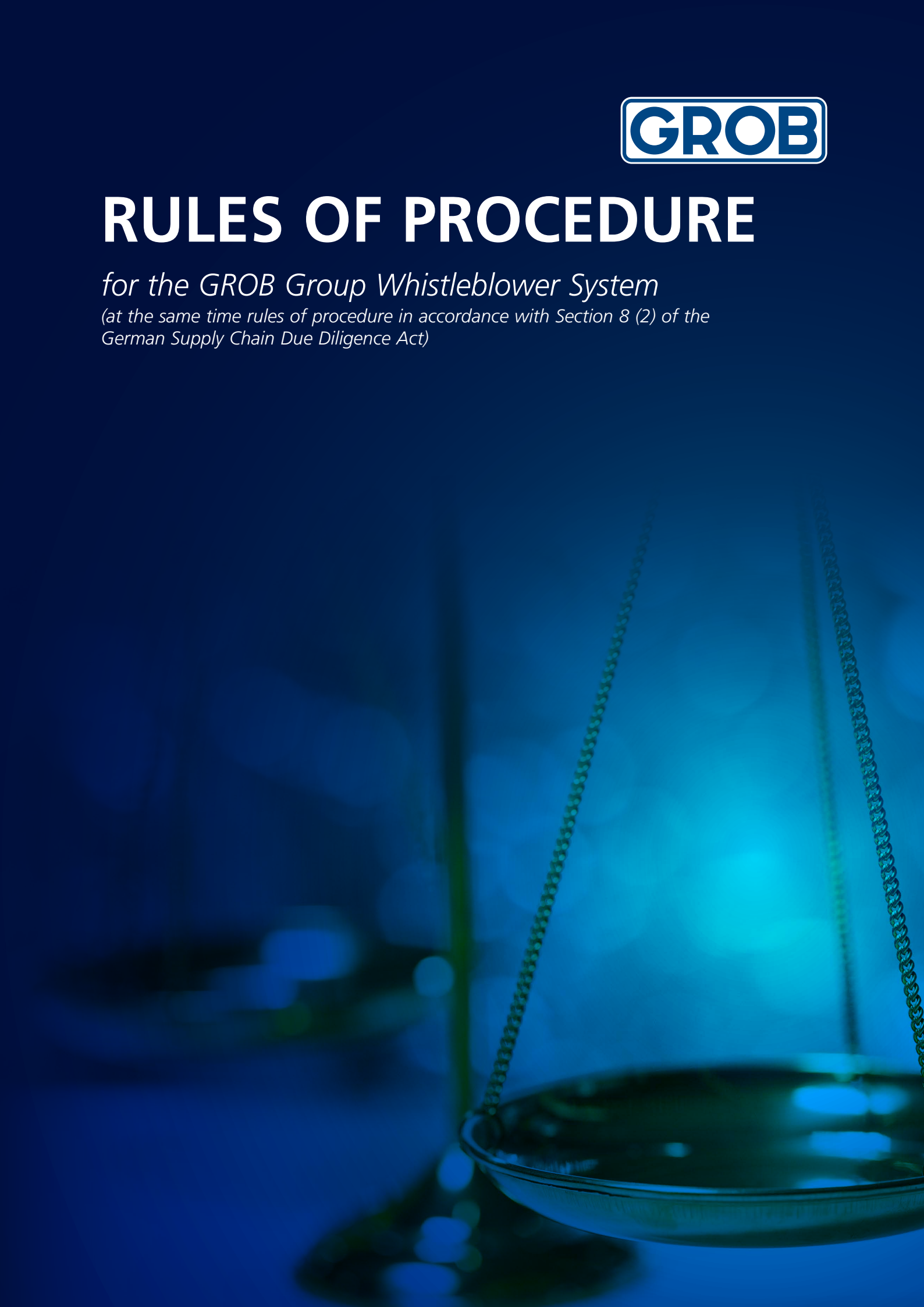
RULES OF PROCEDURE

for the GROB Group Whistleblower System

(at the same time rules of procedure in accordance with Section 8 (2) of the German Supply Chain Due Diligence Act)



GROB Whistleblower System

CONTENTS

GROB Whistleblower System

1. INTRODUCTION

We at GROB are convinced: Entrepreneurial success requires a stable foundation characterized by a clear commitment to legal compliance and ethically impeccable conduct at all times. With our Compliance Management System, we want to **PREVENT** violations of these principles within the GROB Group, **DETECT** misconduct directed against them and **STOP** this through targeted measures.

Our whistleblower system (hereinafter also referred to as the reporting platform) plays an essential role in this. Only those who are aware of possible weaknesses in their organization are in a position to independently correct any misconduct that has occurred and improve processes for the future. However, even a fully developed Compliance Management System cannot prevent the occurrence of new, previously unknown compliance risks, nor can it prevent all breaches of rules by individuals – whether intentional or not. We therefore see our whistleblowing system as an **EARLY WARNING SYSTEM** that helps us to live up to our corporate responsibility.

With this in mind, we want to encourage all employees, business partners and anyone else who feels included to report justified suspicions of possible wrongdoing, misconduct and irregularities within the GROB Group. In taking this step, we wish to support potential whistleblowers in the best possible way. These procedure rules are intended as a **GUIDE** to proactively answer questions that may arise in the run-up to an intended submission, thus providing potential whistleblowers with sufficient security.

2. SCOPE OF APPLICATION

These procedure rules govern GROB-WERKE GmbH & Co. KG with its registered office in Mindelheim and its subsidiaries ("GROB Group") the function of the company's own whistleblower system, and at the same time are intended to ensure transparent presentation of the complaints procedure within the meaning of Section 8 (2) of the German Supply Chain Due Diligence Act (German 'Lieferkettensorgfaltspflichtengesetz' or LkSG).

The procedure rules for the GROB Group's whistleblower system apply upon publication.

3. GROB WHISTLE-BLOWER SYSTEM

3.1. What information can be reported?

The whistleblower system can be used for submission if information or well-founded suspicions of actual or potential violations have been obtained in the professional context. The whistleblower system relates in particular to the following compliance-relevant risks or violations:

- Bribery, corruption and kickbacks
- Embezzlement, misappropriation and theft
- Violations of competition and antitrust laws
- Conflicts of interest
- Suspected money laundering
- Sexual harassment, physical or psychological violence, discrimination
- Violations of human rights, labor and social standards
- Violations of environmental obligations
- Violations of data protection and IT security
- Violations of product safety
- Sanctions violations

In this context, whether the alleged violation was committed by a company, an employee, a business partner or a direct or indirect supplier of the GROB Group is irrelevant. Only a professional context to the GROB Group must exist.

3.2. Who can submit a report?

Our whistleblower system can be used by all persons who have perceived a violation of or a risk for one of the aforementioned compliance-relevant risks or violations. In factual terms, our whistleblowing system is aimed at:

- All employees of the GROB Group
- Employees of suppliers, customers and business and cooperation partners of the GROB Group
- Other third parties

In this context, we would like to expressly point out that it is not necessary to be personally affected in order to be able to submit a report. On the contrary: Even persons who have only observed or heard about a relevant event can submit reports.

3.3. What information is not wanted?

We ask all whistleblowers to use the whistleblower portal responsibly. Very important: Our whistleblower system is also open to you in cases of doubt – please use it. We will then initiate comprehensive clarification of the facts and precise legal examination.

Only submissions accusing employees or third parties with malicious intent and against better knowledge are expressly not welcome. Such reports obviously intended to harm, denounce or disparage other persons will not be processed. In such cases, we expressly reserve the right to take any measures, rights and claims against the person providing the information.

4. REPORT SUBMISSION AND FURTHER PROCEDURE

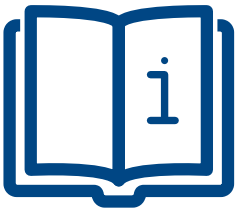
4.1. What channels can be used to submit a report?

Whistleblowers can either contact the Head of Compliance and his compliance team in Mindelheim directly (in person, by telephone or in writing) or send us their report via our digital, web-based reporting platform.

The contact details of the Head of Compliance and his team are publicly available on the company's website in the section *Company* > *Compliance*.

The digital reporting platform can be accessed via the following link:
https://sicher-melden.de/grobgroup.

4.2. How does the digital reporting system work?



The digital reporting platform is operated by the external provider otris software AG, through which the report is transmitted directly to GROB Group's Compliance Team in an encrypted and non-traceable form.

The input form on the digital whistleblower platform is available in **A TOTAL OF EIGHT LANGUAGES** (German, English, French, Spanish, Polish, Italian, Portuguese and Hungarian). Text entries can be made by the whistleblower in any language. The reporting platform can be accessed around the clock.

The digital reporting platform also allows anonymous submission of reports. This means that reports can be submitted without disclosing the identity of the person providing the information. By clicking on the *Submit new report* button, the person submitting the report can set up an anonymous mailbox. In the last step before submission of the report, the person receives individual access information that serves as an access key. The access information consists of a password assigned by the person submitting, and an ID code. With the help of this access information, the person submitting the report can access their anonymous mailbox at any time (*Track report* button). Very important: If the access information is lost, access to the anonymous mailbox cannot be restored!

With the help of the anonymous mailbox, the whistleblower can track the status and processing progress of their report and send further messages with additional information to the recipient of the submission. At the same time, GROB Group's compliance team can communicate with the anonymous whistleblower, for example to ask questions on the facts of the case if necessary, or to transmit messages on the processing status and the outcome of the investigation.

Only if whistleblowers actively remove anonymity will they be asked to provide a name and possible contact information. In this case, the person providing the information is, of course, also free to provide all or only part of the contact data.

In addition, the input form consists of various fields, which are selection fields on the one hand and free text fields on the other. In addition, files such as images or PDF documents can be added as attachments.

4.3. What should be generally observed when submitting a report?

The following principle applies: All information will be processed. However, the more information GROB Group's compliance team receives about the potential misconduct/ grievance, the faster and more effectively the submission can be processed and the harmful behavior can be stopped. The so-called W-questions provide orientation for writing a meaningful submission:

- **WHAT HAPPENED?**
  Concise description of the facts in chronological order.
- **WHO COMMITTED THE VIOLATION?**
  If employees of the GROB Group are affected, indication of the name, position and the GROB Group company concerned, if known. The same applies to affected employees of suppliers and business partners.
- **WHEN DID THE INCIDENT OCCUR? IS THE VIOLATION STILL CONTINUING?**
  If possible, state the date and time or period of the violation.
- **WHERE DID THE VIOLATION OCCUR?**
  Location, department, etc.
- **HOW CAN THE VIOLATION BE PROVEN?**
  Evidence that can be attached to the report, e.g., photos, screenshots, emails, or naming witnesses along with contact information.
- **WHO KNOWS ABOUT THE INCIDENT?**
  Has the incident already been reported elsewhere (e.g., to a supervisor)?

4.4. Who processes incoming reports?

All incoming reports are processed by the compliance team of GROB-WERKE GmbH & Co. KG in Mindelheim. The employees working there under the direction of the Head of Compliance are responsible for receiving, reviewing, investigating and documenting an incoming submission and will take the necessary investigative actions. If necessary, the report is forwarded to the relevant department. Depending on the specific facts of the case, external experts, in particular law firms specializing in certain areas of law, may also be called in on a case-by-case basis.

The members of the compliance team are entrusted with processing reports act impartially and independently. It is also ensured that they can act independently of instructions with regard to their investigative tasks, and that they receive regular training specifically tailored to this task.

4.5. What happens when a report has been submitted?

All incoming submissions – regardless of whether they are submitted directly to the Head of Compliance and his team or whether they are received via the digital reporting platform – are processed in accordance with a defined process:

Acknowledgement of receipt

Upon receipt of a submission, the GROB Group compliance team is informed of the existence of a new report. Provided that the person providing the tip can be contacted – either directly or via the anonymous mailbox – an acknowledgement of receipt will be received within **SEVEN DAYS**. Only if the information is provided anonymously in such a way that it is impossible to contact the person providing the information will there be no confirmation of receipt.

Plausibility check

First, the member of the compliance team responsible for the report carries out an initial evaluation without any results. The aim of this **INITIAL EVALUATION** is to check the plausibility of the content of the report. If necessary, the department concerned is consulted and, if required, the whistleblower is contacted – either directly or via the anonymous mailbox – in order to obtain further information on the course of events.

If the allegation cannot be substantiated by means of further investigations or information from the whistleblower, the case will be closed. The person providing the information will be informed of this.

Investigation

If the suspicion of possible misconduct or a corresponding risk is substantiated during the initial evaluation, the compliance team member responsible for the report will **COMPREHENSIVELY** clarify the facts of the case with the involvement of the department concerned. Here, too, the following applies: If possible and appropriate, the matter is discussed with the person making the submission.

Evaluation & initiation of measures

Based on this, the person providing the information makes an **EVALUATION** of the facts under investigation, develops **FOLLOW-UP MEASURES** in coordination with the Head of Compliance and ensures that they are **IMPLEMENTED** as quickly as possible. If the person making the report is affected by the reported facts, the compliance team will attempt to involve this person as much as possible in the development of proposed solutions.

The follow-up measures can on the one hand be the initiation of **REMEDIAL MEASURES**, which serve to end misconduct that has already actually occurred and to eliminate or at least minimize its extent of damage for the GROB Group itself, its employees, business partners or other third parties. This can have an impact on certain corporate processes, result in personnel measures and, in particular in the case of criminal acts, mean contacting (law enforcement) authorities.

On the other hand, **PREVENTION MEASURES** are developed to prevent the risk of repetition of the misconduct in the future. Existing prevention measures will be reviewed on an as-needed basis based on the current submission and improved as needed.

Conclusion & feedback

The following applies in general: We process all reports as quickly as possible. As a rule, the facts of the case are clarified **WITHIN THREE MONTHS** of confirmation of receipt of the submission. However, the duration of an investigation can vary from case to case, depending on how extensive and complex the facts are. Some investigations take only a few days, while other investigations may take several months.

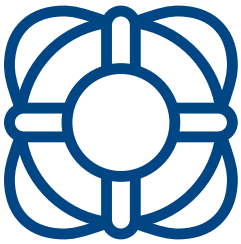
The person making the report can contact the compliance team at any time to find out the status of the report. In any case, feedback will be received on the status quo of the processing or the outcome of the investigation after three months at the latest. Taking into account the applicable data protection regulations and other confidentiality requirements, as well as safeguarding overriding corporate interests, the feedback includes the result of the clarification of the facts, any follow-up measures taken and their effectiveness.

In the event that the suspicion proves to be unfounded in the course of the investigation, the investigation will be discontinued. The person providing the information will be informed of this and will receive an appropriate explanation.

4.6. Documentation & retention

The respective complaint process is documented and stored in accordance with legal requirements.

5. PROTECTION OF THE WHISTLEBLOWER



Whistleblowers who provide information in good faith in order to uncover grievances enjoy special protection within the GROB Group.

IN DETAIL, THIS MEANS:

- Only those persons who are responsible for receiving submissions or taking follow-up action will be aware of the full content of the submission, including the identity of the person providing it (if specified). All submissions will be treated in strict confidence. If third parties are involved in connection with the processing of the tip by the Compliance department – whether employees from the departments concerned or external third parties – they will only receive the information that they absolutely need to process the submission.
- Information on the identity of the persons providing the information may be passed on to the competent bodies (e.g., authorities, courts) if this is required by a court or official order or if there is sufficient suspicion of a criminal offense.
- Named whistleblowers need not fear reprisals such as suspension, dismissal, transfer of tasks, disciplinary measures, discrimination, harassment or similar retaliation on the part of their employer.
- Employees, suppliers and business partners of the GROB Group as well as other third parties must expect consequences if they expose whistleblowers to retaliation. Persons who observe indications of such retaliatory measures should contact the Head of Compliance immediately. The Head of Compliance will decide on the necessary measures to stop any retaliatory actions. Possible measures include, for example, civil and/or criminal prosecution of retaliatory actions, sanctions under employment law (e.g. warning, termination) and termination of contractual relationships.

6. PROTECTION OF THE ACCUSED PERSON

The rights of the person affected or accused by the submission are also protected. The presumption of innocence under the rule of law applies until proven otherwise.

7. DATA PROTECTION

Compliance with statutory retention requirements and data protection regulations is ensured by the Head of Compliance in close cooperation with the GROB Group's Data Protection Officer. The personal data collected is limited to details of the identity, function and contact information of the persons providing the information and persons affected (if specified), as well as other personal data that is absolutely necessary for processing the matter. In addition, only reported facts, processing details, follow-up of the report and test reports are retained.

8. COSTS

The person providing the information does incurs **NO COSTS** by submitting the information. This also applies to the submission of the report via the digital reporting platform. Only their own costs (e.g. general internet and telephone charges) have to be borne by whistleblowers themselves.

9. EFFECTIVENESS

The effectiveness of the whistleblower system is reviewed at least once a year and on an ad-hoc basis. If necessary, adjustments will be made to the procedure or to any remedial action taken.

10. THE MOST IMPORTANT THING AT THE END

If you have any doubts about whether or not to submit a report – listen to your gut feeling and take responsibility! The more people actively respond to misconduct and grievances, the more effective our compliance organization is!