Guideline for Whistleblower System

1. Preamble

On December 16, 2019, the EU Directive on the Protection of Whistleblowers (EU Whistleblower Directive) came into effect. The EU Whistleblower Directive aims to enhance the protection of whistleblowers. Accordingly, companies with 50 or more employees are required to establish and operate a whistleblower system. For this reason, each member state, including Germany, is obliged to transpose the requirements of the EU Whistleblower Directive into national law. Germany has fulfilled this obligation by adopting the so-called Whistleblower Protection Act (HinSchG). The "Processing of personal data, including the exchange or transmission of personal data" must always comply with the requirements of the General Data Protection Regulation (GDPR).

An internal procedural order transparently describes the corresponding internal procedural guidelines and steps within the provided technical facility for reporting. The definitions can be found in the annex to this directive. Further options for submitting a report and important information on terms, etc., are presented below. Questions and additional information can be directed to the contact point and/or contact person as indicated in **13.3.**

2. Introduction

Openness and integrity are crucial in our interactions. Investigating crimes and supporting the organization in addressing concerns or incidents are important to us. Therefore, we welcome being informed about any unlawful behavior within our company to investigate such conduct and take necessary measures. We encourage everyone whether employees, former colleagues, customers, suppliers, or third parties to report violations of the law. Any unlawful actions are strictly prohibited under any circumstances.

In accordance with our internal guidelines, we have defined and established our values, principles, and policies for the entire organization concerning interactions with customers, business partners, suppliers, employees, etc. This directive, within the compliance organization, aims to create the framework for reporting potential violations to specific individuals and through an electronic whistleblower system. This directive should ensure adequate consideration of the legitimate interests of the company, whistleblowers, affected individuals, and the public.

Furthermore, in technical and organizational terms, this directive should ensure that reports of violations of laws and internal policies are received, processed, stored, shared, and archived in accordance with internal guidelines and considering the required confidentiality.

3. Scope

The following rules are intended to support our employees, management, as well as our business partners, customers, suppliers, etc., in recognizing, reporting, and eliminating possible misconduct. This directive outlines cases and ways in which potential issues can be reported. Additionally, this directive clarifies how to handle such reports. Whistleblowers should not fear sanctions or other reprisals for making a good-faith report. We also ensure maximum confidentiality for whistleblowers, contributing to building trust and encouraging everyone to participate. Consequently, you play a valuable role in helping us collectively meet our high standards.

4. Purpose of the Directive

The aim of this directive is the implementation and utilization of an internal whistleblower system, which contributes to the detection and clarification of operational misconduct, harmful behaviour, economic crime, etc., as well as the protection of our employees, business partners, customers, etc. Simultaneously, this directive protects the whistleblower and the affected person.

5. Application Scope

The scope according to § 2 of the Whistleblower Protection Act includes the reporting and disclosure of information about:

- Violations that are punishable by law
- Violations that are subject to fines, insofar as the violated provision serves the protection of life, body, health, or the protection of the rights of employees or their representative bodies,
- Other violations of federal and state regulations as well as directly applicable legal acts of the European Union and the European Atomic Energy Community (e.g., combating money laundering and terrorism financing, product safety, environmental protection, food safety, consumer rights, privacy protection in electronic communication, protection of personal data, information technology security, accounting including bookkeeping, public procurement, etc.)

6. Reporting Entities and Reporting Procedures

6.1 Reporting Entities

All individuals working for our company or in contact with us in the course of their professional activities or gaining information about a violation (hereinafter referred to as "reporting person") are eligible to report. This includes, for example, current, future, or former employees or executives of our corporate group, our business partners, customers, suppliers, freelance workers, interns, or members of the general public (third parties). No one is obliged to submit a report under this directive.

6.2 Submission of Reports (Anonymity)

All whistleblowers are encouraged to report known misconduct, misbehaviour, hazards, etc., in accordance with this directive or information about violations openly and directly, providing their contact details if there is a reasonable suspicion of a violation.

Whistleblowers have the option to submit an anonymous report. Anonymity may need to be lifted in individual cases during investigations. The necessity of lifting anonymity will be communicated to the individual concerned as required. However, actual lifting can only occur with the assistance and consent of the whistleblower.

6.3 Reasonable Suspicion

Not in all cases will it be clearly apparent to the whistleblower whether a specific action or behaviour should be reported according to the principles of this directive.

Therefore, whistleblowers should report only those cases where they have reasonable grounds to believe that the reported information about the violation was true at the time of the violation,

and they have a reasonable suspicion that an incident relevant to this directive occurred. Whistleblowers should always refer to this directive in their reports.

Reports that do not meet the requirements of this directive will not be processed. Whistleblowers will be notified of this outcome. Legal consequences or sanctions against the whistleblower will not result from submitting a report in good faith, even if the report is ultimately not substantiated.

6.4 Specific and Coherent Reports

Each report should be as specific as possible. The whistleblower should present the recipient with detailed information about the matter to be reported, allowing them to assess the situation accurately. In this context, the background, course of events, reason for the report, as well as names, dates, locations, and other relevant information should be provided. The extent of information shared is at the discretion of the whistleblower. If available, documents supporting the report should be submitted. Personal experiences, potential biases, or subjective opinions should be clearly identified as such.

The whistleblower is not generally obligated to conduct their own investigations; an exception may apply if they are contractually obligated to do so as part of their employment agreement.

7. Internal and External Reporting Channels; Submission of Reports

Whistleblowers have various options to contact a responsible party or effectively report an issue. A report can be communicated to the internal reporting channel, i.e., the internal reporting system ("Internal Report"). Alternatively, the whistleblower can also contact an external reporting channel (relevant authorities), such as the police or a data protection supervisory authority ("External Report"). It is advisable to consider personal interests as well as the interests of the involved individuals and the company when deciding on the appropriate procedure for reporting violations, as described below.

7.1 Contacting Representatives

The first point of contact should ideally be the supervisor or the directly responsible person. This is generally the simplest way to address a problem related to the work environment, clarify misunderstandings, and ensure a positive and open working atmosphere. If the matter is substantiated, the contact person, in consultation with the whistleblower, will initiate further steps.

If, for factual or personal reasons, it is unreasonable or impractical for the whistleblower to report to their supervisor, they may also directly contact the management, the head of the local human resources department, or the head of the compliance department as their point of contact. The same applies if the whistleblower believes that the supervisor is not handling the report properly. Regardless, the option to report to the internal reporting channel is available.

7.2 Reporting to the Internal Reporting Channel via the Digital Whistleblower System

Internal reporting ensures that information about violations reaches individuals closest to the cause of the violation, enabling them to investigate and rectify the problem. Whistleblowers should prefer reporting to the internal reporting channel in cases where effective internal action can be taken against the violation, and they do not fear reprisals.

The whistleblower should assess the appropriate level on a case-by-case basis. Reporting to the whistleblower system is particularly advisable when internal communication seems

unreasonable or if the whistleblower believes that their report will not be handled properly internally.

The whistleblower has the option to submit reports at any time through the internal digital whistleblower system, which is appropriately protected and confidential. Further details can be found in the internal procedural regulations for the whistleblower system. Our internal reporting channel is established with an external and independent service provider based in Germany, ensuring the necessary independence and expertise.

7.3 Reporting to External Reporting Channels

The whistleblower also has the option to report to an external reporting channel. It is recommended to carefully weigh all information about the violation and consider whether an internal or external report should be made. In this case, the whistleblower can report the violation to the relevant authorities, such as law enforcement, regulatory, financial, health, or data protection authorities. Such a report should be made, especially if it is legally required, there is a significant public interest, or there is an imminent danger.

In case of imminent danger, priority should be given to informing authorities with emergency powers (police, fire department, etc.). The whistleblower should ensure that the potential negative consequences of the external report for the company and the individuals involved are minimized. The external entity receiving the information must be capable of taking effective steps against the suspected violation.

8. Procedure Following Receipt of a Report

The internal reporting channel confirms the receipt of a report to the whistleblower no later than seven days after receiving it. The internal reporting channel examines whether the reported violation falls within the substantive scope of the Whistleblower Protection Act.

The internal reporting channel maintains contact with the whistleblower and assesses the validity of the received report. Additionally, it may request further information from the whistleblower if necessary.

The internal reporting channel takes appropriate follow-up measures in accordance with § 18 of the Whistleblower Protection Act. These follow-up measures may include:

- Conducting internal investigations at the employer or within the respective organizational unit and contacting affected individuals and work units.
- Referring the whistleblower to other competent authorities.
- Closing the process due to a lack of evidence or other reasons.
- Transferring the process for further investigations to a unit within the employer or the respective organizational unit responsible for internal investigations or to a competent authority.

If the receiving entity believes that further investigations are warranted, it documents this and forwards the information to the internally responsible entity within the company. This entity then conducts internal investigations.

The name of the whistleblower is only disclosed to the company if the whistleblower has given prior consent, and if this is necessary for the follow-up measures.

Feedback to the whistleblower is provided within a maximum of three months after confirming the receipt of the report.

If a report is found to be false or cannot be sufficiently supported with facts, this is documented, and the process is immediately terminated. No consequences shall arise for an individual who was the subject of the report, and the incident is not documented in the personnel file.

9. Documentation of Reports

Individuals responsible for receiving reports in an internal reporting channel document all incoming reports in a permanently accessible manner, adhering to confidentiality requirements. Written and electronic reports are securely stored or saved in our digital reporting system with restricted access.

For oral reports, the following applies in accordance with the Whistleblower Protection Act:

- With the whistleblower's consent, oral reports (e.g., via telephone) are permanently and retrievably recorded in an audio recording. Alternatively, a complete and accurate transcript of the conversation can be created by the contact person.
- If no audio recording of the oral report is made, a meeting transcript can be prepared by the contact person with the whistleblower's consent.

For in-person meetings, the following applies in accordance with the Whistleblower Protection Act:

- If a meeting with the whistleblower takes place, with the whistleblower's consent, an audio recording can be made, and it is permanently and retrievably stored. Alternatively, a meeting transcript can be prepared.

The whistleblower must have the opportunity to review, correct if necessary, and confirm transcripts or records of oral reports or in-person meetings through their signature.

10. Protection of the Whistleblower

Every whistleblower who makes a report in good faith or cooperates in the investigation of a corresponding suspicion should not anticipate negative consequences or reprisals solely due to the act of reporting or participating in the reporting process (e.g., suspension, termination, demotion, reassignment, poor evaluations, disciplinary actions, or discrimination). Likewise, the threat or attempt of reprisals is not permissible.

This protection extends to intermediaries, third parties associated with the whistleblower, and individuals or entities related to the whistleblower in a professional context, such as companies owned by the whistleblower, those for whom they work, or those with whom they have professional connections.

If, despite the aforementioned prohibition, such an incident occurs, it can be reported through the designated reporting channels. The company does not tolerate any form of disadvantage, discrimination, harassment, or similar actions. We examine the circumstances of each case and take temporary or permanent measures to protect the whistleblower and others while safeguarding the interests of the company.

Any employee or supervisor who violates this prohibition of reprisals may face disciplinary actions, which, in extreme cases, could lead to termination.

Whistleblowers who knowingly misuse the whistleblower reporting system for false reports may face disciplinary measures. Additionally, actions such as manipulating, concealing, or breaching agreements regarding confidentiality within the whistleblower system may result in disciplinary measures. Possible measures include warnings or termination. Furthermore, such actions may have civil or criminal consequences.

11. Protection of the Affected Person

11.1 Contact and Hearing

In the case of an internal investigation as a follow-up measure by the internal reporting office, the affected person must be contacted and given an opportunity to be heard before conclusions are drawn at the end of the process described under Section 8, with the person being named.

11.2 Information to the Affected Person

Every person affected by a report will be notified in due course and in accordance with data protection regulations about the allegations made against them, unless such notification would significantly impede the progress of the process for determining the facts or the implementation of follow-up measures. Notification will be made no later than upon the completion of the investigations or when the investigations can no longer be jeopardized.

The name of the whistleblower will only be disclosed if the whistleblower has given prior consent and if this is necessary for the follow-up measures.

12. Data Protection and Confidentiality

Within the framework of this process, personal data is collected and stored. The handling of this data is carried out in accordance with the applicable data protection laws and internal guidelines on data protection.

The internal reporting office is authorized to process personal data as far as it is necessary to fulfil its tasks. This particularly applies to special categories of personal data according to Article 9 of the GDPR.

Only the data objectively necessary for the purposes of this policy will be processed. The collected data will be used exclusively for the purposes described in this policy. The provision of data is done especially to ensure the company's legal obligations and compliance within the company.

We assure all informants of confidential handling. This means that the identity of the reporting person, the identity of individuals mentioned in a report, and the identity of other persons mentioned in the report will not be disclosed to others except those responsible for receiving reports or carrying out any subsequent actions. Deviating from this principle, information about the identity of a reporting person or other circumstances allowing conclusions about this person's identity may be disclosed under the following circumstances:

- In criminal proceedings at the request of law enforcement authorities
- Due to an order in an administrative procedure
- Including administrative fine proceedings
- Due to a court decision
- Due to a procedure of the Federal Financial Supervisory Authority as an external reporting office or the Federal Cartel Office as an external reporting office

In such cases, the informant will be informed in advance about the disclosure. This is waived if the law enforcement authority, the relevant administrative authority, or the court of the respective reporting office has communicated that the information would jeopardize the corresponding investigations, examinations, or legal proceedings.

Furthermore, information about the identity of the reporting person or other circumstances allowing conclusions about this person's identity may be disclosed if:

- The disclosure is necessary for subsequent actions.
- The reporting person has given prior consent to the disclosure.

13. Information, Training, Points of Contact

13.1 Accessible Information/Guidance on the Policy

13.1 Accessible Information/Guidance on the Policy

This policy and its associated internal procedural guidelines will be published through the usual corporate channels (intranet, notice boards, etc.) and communicated to all employees. Employees without intranet access will receive a written copy, which can also be requested from the Human Resources department at any time.

13.2 Employee Training

The company is committed to training all employees on the whistleblowing system. All employees are obligated to complete the training sessions offered by the company on the whistleblowing system.

13.3 Points of Contact

For questions, comments, etc., regarding the provisions of this policy, please contact the following points of contact:

- Internal Reporting Office
- Human Resources Department
- Project Support " rotection of Whistleblowers"

13.4. Violation of this Policy

In case of a violation of this policy, both the whistleblower and the affected individual can contact the internal points of contact or the internal reporting office.

14. Responsibilities and Implementation

The executive management oversees the implementation of the policy. They review, among other things, the effectiveness of measures taken in response to a suspicion raised in accordance with this policy.

The executive management may designate positions within the company to assist in the oversight process.

Worms, 21.12.23

CEO

Attachment to the Definitions

Whistleblower (Reporting Person)

An individual who, in connection with their professional activities or in anticipation of professional activities, has acquired information about violations and reports or discloses such information to the reporting channels provided for by the Whistleblower Protection Act.

Affected Person

A natural person who is the subject of a report or disclosure, as well as any other person affected by a report or disclosure.

Violations

Actions or omissions within the scope of professional, entrepreneurial, or service activities that are unlawful and concern regulations or legal areas falling within the material scope according to § 2 of the Whistleblower Protection Act.

Information about Violations

Well-founded suspicions or knowledge of actual or possible violations that have already occurred or are very likely to occur at the employer where the whistleblower is or was active or at another entity with which the whistleblower has been in contact due to their professional activities, as well as attempts to conceal such violations.

Report

Communication of information about violations to the internal reporting channel or external reporting channels.

Disclosure

Making information about violations accessible to the public.

Reprisals (Disadvantages)

Actions or omissions related to professional activities that are a response to a report or disclosure and result in or may result in unjustified disadvantages to the whistleblower.

Feedback

Communication to the whistleblower regarding planned and already taken follow-up measures, as well as the reasons for these follow-up measures.

Follow-up Measures

Measures taken by an internal reporting channel according to § 18 of the Whistleblower Protection Act or by an external reporting channel according to § 29 of the Whistleblower Protection Act to examine the validity of a report, proceed against the reported violation, or conclude the process.

Internal Reporting Channel

A channel established and operated by the employer for internal reports, to which employees can turn.