Rules of Procedure Whistleblower System and Data Protection Notice

Table of contents

1. Introduction

Business integrity is the basis for the relationship between LEONHARD KURZ Stiftung & Co. KG and its affiliated companies (hereinafter referred to as **'KURZ'**) with their social environment, customers, suppliers and employees.

KURZ is particularly committed to respecting human rights and protecting the environment. KURZ takes appropriate and effective measures to identify and verify human rights and environmental risks in its own business area and in the entire supply chain and to prevent the realization of risks. The human rights and environmental due diligence obligations include the establishment of an effective complaints procedure through which whistleblowers can report violations, risks and other issues.

KURZ has a whistleblower system (hereinafter referred to as **'KURZ Incident Reporting'**). These rules of procedure explain the process of submitting and processing incoming reports via KURZ Incident Reporting. It sets out how KURZ Incident Reporting be accessed, who responsible for KURZ Incident Reporting, what the specific process looks like once a report has been received and what measures are taken to protect the whistleblower.

KURZ Incident Reporting aims to enable whistleblowers* to contact us easily and securely to report complaints and information about potential or suspected misconduct, grievances, infringements or violations (hereinafter referred to as **'Report'**). Through this procedure, misconduct, in particular human rights and environmental violations and risks in the supply chain, can be identified at an early stage and violations that have occurred can be minimized and eliminated, thus safeguarding the corporate integrity of KURZ.

2. Scope of application of the whistleblower system

KURZ Incident Reporting is available to employees* of KURZ, business partners of KURZ and third parties (e.g. representatives and employees of customers, suppliers, etc.) (hereinafter referred to as **'Whistleblower'**) worldwide.

The KURZ whistleblower system refers to Reports on the following topics:

- **Anti-competitive actions and anti-trust violations**
- **Violation of internal rules of conduct**
- **Violations of environmental protection regulations or occupational safety and health regulations**
- **Violations of IT security guidelines**
- **Discrimination / Harassment / Bullying**
- **Violations of social standards and human rights**

*For reasons of better readability, the simultaneous use of the language forms male, female and diverse (m/f/d) is dispensed with. All personal designations apply equally to all genders.

3. Options for submitting a Report

KURZ Incident Reporting includes the option of submitting a Report via the digital software solution ‘KURZ Incident Reporting’, which can be used in four languages. Reports can also be submitted completely anonymously.

On the other hand, Reports can be submitted via the following additional channels:
By telephone, by e-mail, by post or in the form of a personal meeting.
The contact information can be found on the respective KURZ homepage
(e.g. www.kurz-world.com/en/about-kurz/compliance).

Whistleblowers have the opportunity to add and correct their Report at any time.

Costs are incurred when contacting us by telephone or post in accordance with the generally applicable fees. There are no costs for contacting us via the digital software solution or by e-mail.

If the Whistleblower wishes to meet in person, this can be arranged with a representative of the compliance organization within a reasonable period of time. With the consent of the Whistleblower, the meeting can also take place by means of video transmission (e.g. MS Teams, ZOOM etc.).

Telephone contact is possible during KURZ's normal business hours:
Mon – Fri between 9:00 a.m – 5:00 p.m (CET).

4. Procedure

1. Receipt of the Report
Receipt is confirmed to the Whistleblower, if there is a possibility of contact, and appropriately documented.

2. Checking the Report
The Report is reviewed and the further procedure and responsibilities are determined. During processing, Reports are prioritized in terms of their priority, completeness or relevance of the information. At the same time, the risk of the whistleblower's protection being compromised is assessed and the protection and support to be provided for the Whistleblower and other parties involved is evaluated.

3. Clarification of facts
The facts on which the report is based are discussed with the Whistleblower - insofar as contact is possible - with the aim of gaining a better understanding of the facts. Even if the facts are assessed as implausible or the facts are not confirmed, the Whistleblower will receive feedback no later than three months after receipt of the Report.

4. Preventive and/or remedial measures
The Whistleblower will be asked about their expectations with regard to possible preventive or remedial measures.

5. Investigation
The facts of the Report are investigated. If the facts on which the Report is based are confirmed, preventive and/or remedial measures are defined. If a violation of human rights or environmental obligations is identified, remedial measures are initiated immediately. If a human rights or environmental risk arises from a Report without a violation having occurred, preventive measures are initiated.

6. Result
The defined preventive and/or corrective measures are implemented and followed up.

7. Review and conclusion
The result achieved by the investigation and the preventive and/or corrective measures are evaluated.

5. Reviewing the effectiveness of the whistleblower system

The effectiveness of the whistleblower system is reviewed annually and on an ad hoc basis. If necessary, adjustments are made to the procedure or corrective measures taken.

6. Recipients of Reports

The receipt and initial validation of reports is carried out by the Group Compliance Officer and the Deputy Group Compliance Officer (hereinafter referred to as the **'Compliance Organization'**) at the KURZ Group headquarters in Fuerth, Germany. The employees of the Compliance Organization are part of KURZ's central services and report directly to the CEO of the Leonhard Kurz Foundation. The independence of the employees of the Compliance Organization is guaranteed in the performance of their duties. Depending on the subject of the Report, the relevant department will examine the Report and clarify the facts. However, communication with the Whistleblower, in particular feedback, is always provided by the Compliance Organization.

7. Protection against discrimination and punishment of the whistleblower

In any case, Whistleblowers are protected from unjustified discrimination and punishment.

As recipients of Reports, the employees of the Compliance Organization are legally and contractually obliged to maintain the confidentiality of the identity of the Whistleblower. The members of the Compliance Organization must handle Reports confidentially and impartially.

If a Report is submitted via KURZ Incident Reporting, the Whistleblower is additionally protected by the fact that Reports can be submitted easily, securely and anonymously. The system ensures that all data and information, especially the identity of the Whistleblower, can be treated confidentially.

The KURZ Incident Reporting application is operated on dedicated servers in a high-security data center in Germany. The administration and maintenance of the servers is the sole responsibility of an external service provider, who has no right of access to the correspondence with the Whistleblowers. The data center is secured by an actively controlled firewall. Only the services required for application and maintenance are installed on the server. Data transfer started from the inside and direct access to the server are not possible. The database is secured with a further security level by a firewall that only responds to requests from the local system.

8. Submission of blatantly false reports and misuse of the whistleblower system

Reports that are obviously false will be rejected at any time. It should be noted that such Reports may give rise to claims for damages and may be prosecuted.

9. Data protection notice

KURZ takes the issue of data protection and confidentiality very seriously and complies with the provisions of the EU General Data Protection Regulation (EU GDPR) and applicable national data protection regulations. Please read this data protection information carefully before submitting a Report. KURZ ensures that the confidentiality of the identity and the reported misconduct is maintained.

Purpose of the whistleblower system and legal basis
The whistleblower system (KURZ Incident Reporting) serves to receive, process and manage Reports on violations of the compliance requirements of LEONHARD KURZ Stiftung & Co. KG and its group companies in a secure and confidential manner. The processing of personal data in the context of KURZ Incident Reporting is based on the legal obligation of the German Whistleblower Protection Act and serves to detect, eliminate and prevent grievances and thus to avert damage that could arise for LEONHARD KURZ Stiftung & Co KG and its group companies as well as their employees and customers. The legal basis for this processing of personal data is Article 6 para. 1 sentence 1 lit. c EU GDPR in conjunction with section 10 HinSchG, in Austria: Section 8 HSchG. The personal data is processed exclusively for the purpose of reviewing and processing the Whistleblower's Report.

Responsible body
The body responsible for data protection in the whistleblower system is
1. LEONHARD KURZ Stiftung & Co. KG and
2. its subsidiaries
as autonomously responsible bodies on both sides. The whistleblower system is operated by a specialized company, EQS Group AG, Bayreuther Str. 35, 10789 Berlin, Germany, on behalf of KURZ. A data processing agreement has been concluded with EQS Group AG, Bayreuther Str. 35, 10789 Berlin, Germany, in accordance with Art. 28 GDPR.

Personal data and information entered into the whistleblower system are stored in a database operated by EQS Group AG in a high-security data center. Access to the data is only possible for KURZ. EQS Group AG and other third parties have no access to the data. This is guaranteed in the certified process by comprehensive technical and organizational measures.

All data is encrypted and stored with multi-level password protection and is subject to an authorization concept, so that access is restricted to a very narrow circle of recipients expressly authorized by KURZ.

If KURZ is legally obliged to do so (exceptional cases according to § 9 HinSchG), data will be passed on to external bodies such as authorities or public prosecutors.

KURZ has appointed a data protection officer. Inquiries regarding data protection at MKM Datenschutz GmbH can be sent to DSB@Kurz.de.

Type of personal data collected
The whistleblower system is used on a voluntary basis. If you submit a Report via the whistleblower system, we collect the following personal data and information:
· Name, if your identity is disclosed,
· Employment relationship with KURZ and
· where applicable, names of persons and other personal data of the persons named in a Report.

Confidential treatment of Reports
Incoming Reports are received by a narrow circle of expressly authorized and specially trained employees of the KURZ Compliance Organization and is always treated confidentially. The employees of the KURZ Compliance Organization examine the facts of the case and, if necessary, carry out further case-related clarification of the facts.

In the course of processing a Report or as part of a special investigation, it may be necessary to pass on Reports to other employees of KURZ or employees of other group companies, e.g. if the Report relates to group companies. The latter may also have their registered office in countries outside the European Union or the European Economic Area, in which different regulations for the protection of personal data may exist. KURZ always ensures that the relevant data protection regulations are complied with when passing on a Report.

Every person who has access to the Report is obliged to maintain confidentiality.

Notice to the accused person
In principle, we are legally obliged to inform the accused persons that we have received a Report about them as soon as this notice no longer jeopardizes the follow-up of the Report. Your identity as a Whistleblower will not be disclosed – as far as legally permissible.

Rights of data subjects
Under European data protection law, you and the persons named in the Report have the right to information, rectification, erasure, restriction of processing, the right to data portability and the

right to object to the processing of your personal data. However, the right to information about the stored data in the context of whistleblower protection only exists if the information would not reveal any information that must be kept secret due to the overriding legitimate interests of a third party. If the right to object is exercised, KURZ will immediately check the extent to which the stored data is still required for the processing of a Report. Data that is no longer required will be deleted immediately.

You also have the right to lodge a complaint with a supervisory authority. The competent supervisory authority for LEONHARD KURZ Stiftung & Co KG is:
Bavarian State Office for Data Protection Supervision (BayLDA)
Promenade 18
91522 Ansbach
Phone: +49 (0) 981 180093-0
E-Mail: poststelle@lda.bayern.de

Retention period of personal data
In the whistleblower system, data can be processed in connection with very different legal circumstances. The retention periods and the resulting deletion periods for personal data result either from the law or the necessity of processing for the specific purpose. The periods can be between three years and ten years. If you require more detailed information in this regard, please contact the data protection officer in individual cases.

Use of the whistleblower system
Communication between your computer and the whistleblowing system takes place via an encrypted connection (SSL). The IP address of your computer is not stored while you are using the whistleblower portal. To maintain the connection between your computer and KURZ Incident Reporting, a cookie is stored on your computer that only contains the session ID (so-called session cookie). The cookie is only valid until the end of your session and becomes invalid when you close your browser.

You have the option of setting up a protected mailbox in the whistleblower system with a pseudonym/user name and password of your choice. In this way, you can send reports to the responsible KURZ employee by name or anonymously and securely. In this system, the data is stored exclusively in the whistleblower system and is therefore particularly secure; it is not a normal e-mail communication.

Sending attachments
When submitting a Report or sending a supplement, you have the option of sending attachments to the responsible KURZ employee. If you wish to submit a Report anonymously, please note the following security advice: Files may contain hidden personal data that could jeopardize your anonymity. Remove this data before sending. If you are unable to remove this data or are unsure, copy the text of your attachment to the text of your Report or send the printed document anonymously to the address listed in the footer, quoting the reference number you receive at the end of the reporting process.

E-Mail: Compliance@kurz.de

LEONHARD KURZ Stiftung & Co. KG
Schwabacher Str. 482
90763 Fuerth/Germany
Phone: +49 911 71 41-0
www.kurz-world.com

Version 2.0 2025/01

Follow us on: