



Rules of Procedure Whistleblower System

Scope of the Whistleblower System

The whistleblower system of LEONHARD KURZ Stiftung & Co. KG and its affiliated companies (hereinafter referred to as “KURZ”) refers to complaints and reports (hereinafter referred to as “Reports”) on the following topics:

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

The KURZ Whistleblower System 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”).

Channels to give a Report

The KURZ whistleblower system includes a digital software solution called “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 phone, by e-mail, and by mail. The contact information can be found on the respective KURZ homepage:

www.kurz.de/unternehmen/Hinweisgebersystem/

Costs arise when contacting by telephone and mail according to the generally applicable fees. There are no costs for contacting us by e-mail. Telephone contact is possible during KURZ’s normal business hours: Mon – Fri between 8:00 – 17:00 (CET).

*For reasons of better readability, the language forms male, female and diverse (m/f/d) are not used simultaneously. All references to persons apply equally to all genders.

Procedure

1. Receipt of Report

Receipt will be confirmed to the Whistleblower, if contact is possible, and appropriately documented.

2. Checking the Report

The Report will be examined and the further procedure and responsibilities will be determined.

3. Clarification of the Facts

The facts underlying the Report are discussed with the Whistleblower with the aim of gaining a better understanding of the background. Even if the facts are assessed as implausible or the facts can not be confirmed, the Whistleblower will receive feedback no later than three months after receipt of the Report.

4. Preventive and/or Corrective Actions

The Whistleblower is asked about his or her expectations regarding possible preventive or corrective action.

5. Investigation

The facts of the case are investigated. If they are confirmed, preventive and/or corrective actions are determined.

6. Result

The defined preventive and/or corrective actions are implemented and followed up.

7. Review and Conclusion

The result achieved by the investigation and the preventive and/or corrective actions are evaluated.

Review of 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 actions taken.

Recipient of Reports

Reports are received by the Compliance Organization at KURZ's corporate headquarters in Fürth. The employees of the Compliance Organization are part of KURZ's Central Services and report directly to the CEO.

Protection against Disadvantages and Punishment of the Whistleblower

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

As recipients of Reports, the employees of the Compliance Organization are obligated by law and by contract to maintain the confidentiality of the identity of the Whistleblower.

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 exclusive responsibility of an external service provider, who has no right to inspect 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 as well as direct access to the server are not possible. With a further security level, the database is secured by a firewall that only responds to requests from the local system.

Follow us on:



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

Version 1.0 Status 12/2022