

Data Privacy Information Chrono24 Whistleblowing



Upholding Transparency Requirements

This document outlines how we process your personal data when you use the whistleblowing system. Please read the information thoroughly. If you have any questions, our data privacy team will be happy to help.

Entities Responsible for Processing

The entities responsible for processing data in relation to the whistleblowing system are:

- Chrono24 GmbH
Haid-und-Neu-Strasse 18, 76131 Karlsruhe, Germany
- MPN Marketplace Networks GmbH
Haid-und-Neu-Strasse 18, 76131 Karlsruhe, Germany

The companies (hereinafter "Chrono24" or "we") can be reached via email, phone, or fax:

- Email: info@chrono24.com
Tel.: +49 (0)721 96693-0
Fax: +49 (0)721 96693-990

You can contact Chrono24's data privacy officer at the address above (FOA: Data Privacy Department) or at datenschutz@chrono24.com.

You are also welcome to contact our compliance officers with content-related questions at compliance@chrono24.com.

What is the whistleblowing system?

The whistleblowing system allows you to safely and anonymously report potential compliance violations and allows us to process them. You can report violations of laws and violations of our

internal code of conduct using the system. In order to prevent and investigate wrongdoings, as well as to reduce the risk of damages and liability for Chrono24, we may need to process personal data.

What data are processed?

We process both personal and anonymous data when handling reports.

The following information is needed to submit a report:

- The company in which the incident occurred
- The category in which the wrongdoing fits best
- The details of the compliance violation in the text field
- An email address

The first three pieces of information are required to process your report. It is possible that your personal data or those of the offending party may be revealed in the text field. The processing of these data are lawful in accordance with Article 6(1)(f) of the EU General Data Protection Regulation (GDPR). Our legitimate interest required under the GDPR is the discovery of wrongdoings reported via the whistleblowing system. Violations can result in damage to the company's reputation, fines, compensation payments, and other financial losses.

Although you need to provide an email address, your anonymity is protected. We only receive an encrypted version of your email address, which allows us to comply with our legal obligations under Section 17(1)(1) of the German Whistleblower Protection Act and confirm receipt of your report. It is therefore not possible for us to know who you are if you wish to remain anonymous. The legal basis for the collection of your email address is our legal obligations under Article 6(1)(c) GDPR and Section 17(1)(1) of the German Whistleblower Protection Act.

You may also volunteer further information relating to the incident, including:

- The relevant department
- If you work in this department
- When the incident occurred
- If management knows about the incident
- If anyone else knows about the incident
- Who was involved in the compliance violation

By providing us with your personal data, you consent to the processing thereof under Article 6(1)(a) GDPR. The additional information and potential processing of your personal data allow us to process reported incidents more efficiently.

If you voluntarily provide personal data relating to the offending party or other parties involved in the incident, the processing thereof is carried out on the basis of our legitimate interest in accordance with Article 6(1)(f) GDPR. The parties concerned do not have an overriding interest that would hinder the processing, since their rights are protected by adequate measures.

No information about your web browser or your IP address is saved when using the whistleblowing system.

How long are personal data stored?

We are required under Section 11(1) of the German Whistleblower Protection Act to document all tips. The retention period specified under Section 11(5) of the same draft Act is two years from the end of the procedure. All documentation is deleted once this two-year period expires.

Transfer of Data

The tip you provide may be shared internally with Chrono24 Direct GmbH, Chrono24 UK Ltd., and Fratello B.V. These are all Group subsidiaries. Data are transferred for the purposes of investigating compliance violations internally and directly. The corresponding information will only be transferred to the Group company affected by the compliance violation following a plausibility check.

The transfer of personal data is lawful under Article 6(1)(f) GDPR. The legitimate interest required under this clause is the Group-wide and efficient investigation of wrongdoings.

For our whistleblowing system, we use the Suggestion Ox platform operated by Suggestion Ox, Inc. (340 S. Lemon Ave #5601, Walnut, CA 91789, USA). We have signed a data processing agreement with Suggestion Ox, Inc. as laid out in Article 28 GDPR. With this agreement, Suggestion Ox, Inc. guarantee that they process data in accordance with the General Data Protection Regulation and protect the rights of the data subject. Suggestion Ox, Inc. is located in the United States of America. If you are located outside the US, this means the transfer of your email address to a third country. Data transfer to the USA is permitted since we have signed standard data protection clauses as laid out in Article 46(2)(c) GDPR, thus guaranteeing a sufficient level of data protection under Article 46(1) GDPR. Furthermore, Suggestion Ox, Inc. has implemented additional measures to ensure adherence to an appropriate level of data protection.

If you decide to provide names in your report, the people you have named will have a right of access to their personal data in accordance with Article 15 GDPR. This also includes a right to disclosure of the identity of the person who provided the information. However, this right only exists if the interest of the person requesting the information outweighs your interest in confidentiality as a whistleblower. Generally speaking, the preservation of your anonymity as a whistleblower, and thus your interest in confidentiality, prevails, and we do not provide the data subject with any information about you. However, if you have intentionally provided false information about someone, their right of access may prevail.

Rights of the Data Subject

Under the GDPR, data subjects have the following rights:

- The right to withdraw their consent at any time (Article 7(3) GDPR). Data subjects can withdraw their consent by contacting compliance@chrono24.com.
- The right of access (Article 15 GDPR).
- The right to rectification of inaccurate personal data (Article 16 GDPR).
- The right to erasure (Article 17 GDPR).
- The right to restriction of processing (Article 18 GDPR).
- The right to data portability (Article 20 GDPR).
- The right to object (Article 21 GDPR). Data subjects can exercise the right to object by sending an email to compliance@chrono24.com.
- The right to lodge a complaint with a supervisory authority (Article 77 GDPR).