Privacy policy

Privacy policy for the complaints/whistleblower system

INDUS Holding AG, Kölner Straße 32, 51429 Bergisch Gladbach, Germany (hereinafter referred to as "INDUS," "us," "our," and "we") provides the following information in accordance with the General Data Protection Regulation (GDPR) regarding the handling of your personal data when using our complaint/whistleblower system ("SpeakUp").

Purpose of processing

"SpeakUp" enables you to contact us and report compliance and legal violations. The system thus serves the overarching purpose of transmitting reports of potential violations of laws or internal rules in a secure and confidential manner.

With regard to the person making the report, we process personal data for the purpose of identifying and investigating misconduct within the INDUS Group. When you submit a report, you are free to decide whether you wish to do so under your name or anonymously. Please note that we may be required by law to disclose your name to the person you have accused or other affected parties (e.g., witnesses you have named). Please do not include any sensitive personal data in your report, such as ethnic origin, health data, political opinions, religious beliefs, trade union membership, health data, or data on sexual orientation.

Tips can be submitted as text messages and include attachments (such as photos or documents). Reports can also be submitted via voice message. To protect your anonymity, the recorded voice is transcribed into text.

In this case, we may have further questions. These can be sent and answered by both parties via the secure mailbox provided in the SpeakUp system. Access is only possible with a case ID (PIN) and the corresponding password.

In this context, we process personal data in particular to check whether the information provided to us appears plausible and suggests a violation, and to clarify the facts of the matter. Processing may also be carried out on the basis of further clarification for the purpose of exonerating persons who have been wrongly suspected, averting imminent economic and other disadvantages, and asserting and/or enforcing the rights of our company and fulfilling any obligations of our company to cooperate with investigations by law enforcement or other authorities.

Automated decision-making

We assure you that we will examine the case carefully. Decisions are not made automatically by an IT system/AI application, but in each individual case after careful consideration by humans.

Categories of personal data

The following personal data may be processed in this context:

• (Contact) information about the whistleblower

In principle, it is possible to use SpeakUp without providing personal data. Of course, you are free to voluntarily disclose personal data during the process, such as your first and last name, contact details, and whether you are employed by INDUS.

• Case information related to the report

Your personal data (such as
e.g., first name, last name, job title, personally identifiable location and time data, or other information that allows conclusions to be drawn about you/your identity). Furthermore, it is possible that company documents (such as performance records, travel expense reports, logbooks, invoices, and similar documents) that may also contain data relating to you may be processed if they are necessary for clarifying the reported matter.

• System-related data

In the course of the report, system-related data about you will be processed in SpeakUp. It is also possible that information about your behavior when using company communication systems, such as metadata, log data, or even the content of company emails, may be processed if it is necessary for the processing and investigation of the reported incident.

• Special categories of personal data

As a matter of principle, we do not collect any special categories of personal data, such as information on ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, or data on sexual orientation. However, due to the free text fields used to ensure maximum accessibility, it is possible for you to enter such data.

Legal basis for the processing of personal data

The legal basis for the processing of your personal data is, in particular, legal obligations under the Whistleblower Protection Act (Art. 6. para. 1 lit. c GDPR in conjunction with Art. 17 of Directive (EU) 2019/1937 ("EU Whistleblower Directive") and any other national regulations (e.g., with regard to matters relevant to criminal, competition, and labor law) for the implementation of the EU Whistleblower Directive. In accordance with the Whistleblower Directive and the national regulations for its implementation, we are legally obliged to provide a whistleblower system. If a report received concerns an employee of INDUS or an affiliated company, the processing also serves to prevent criminal offenses or other legal violations in connection with the employment relationship. This is based on Art. 6 para. 1 lit. f GDPR. Insofar as the aforementioned special categories of personal data are or become part of the reports or subsequent investigation proceedings, we process them on the basis of Art. 9 (2) lit. b GDPR in conjunction with Art. 9 (2) lit. f) GDPR and applicable national regulations. The processing of your personal data is also based on our legitimate interest (also in relation to third parties) in accordance with Art. 6 (1) sentence 1 lit. f) GDPR

in conjunction with any applicable provisions of national laws on the prevention and detection of criminal offenses, breaches of duty, and other violations, as well as our legitimate interest in averting damage and liability risks for our company. We have a legitimate interest in processing personal data for the prevention and detection of violations within our company, for reviewing the legality of internal processes, and for maintaining the integrity of our company. In particular, reference is made in this regard to the prevention and defense against administrative offenses and criminal offenses within the meaning of
Sections 30 and 130 of the OWiG (German Administrative Offenses Act).

Personal data is also processed within the framework of a whistleblower system (complaints procedure) on the basis of Section 8 of the Supply Chain Due Diligence Act (LkSG), among other things. The complaint procedure enables individuals to report human rights and environmental risks as well as violations of human rights or environmental obligations that have arisen as a result of the economic activities of a company in its own business area or of a direct supplier.

The processing of your identification data as a whistleblower is based on your consent in accordance with Art. 6 (1) (a) GDPR. If you disclose special categories of personal data to us, we will process this data on the basis of your consent (Art. 9 (2) (a) GDPR). The voluntary nature of consent is ensured by the fact that the report can always be made anonymously. You can leave your message anonymously or provide your name and contact details in the free text field.

However, **revocation of consent** can (in certain cases) only take full effect within a limited time frame. This results (in certain cases) from INDUS's obligation under Art. 14 (3) (a) GDPR to inform accused persons and other affected parties (e.g., witnesses) of the allegations made against them and the investigations carried out within one month of receiving the report at the latest, provided that this does not conflict with the purpose of the investigation. The information regularly includes the type of data, the purpose of the processing, the storage period, the identity of the data controller and, if applicable, the identity of the person who provided the information. Once processing/investigation has reached an advanced stage, it is generally no longer possible to discontinue processing or delete the identifying data of the person who provided the information. If information, including names, has been disclosed to the competent authorities or jurisdictions, this information is stored both in our records and with the aforementioned recipients and cannot be deleted without further ado.

Retention periods for personal data

We store your personal data for a period of time that is necessary to process the matter (resulting from your report). The duration of storage depends in particular on the seriousness of the suspicion and the reported breach of duty, if any. Deletion is generally based on the legal requirements for whistleblower protection – regularly 3 years, Section 11 (5) of the Whistleblower Protection Act (HinSchG). Something else applies if applicable legal provisions require something else (for example, in connection with pending court proceedings), in which case the relevant procedural files are regularly retained for 10 years after the conclusion of the proceedings/case.

Technical implementation and security of your data

SpeakUp includes an option for anonymous communication via an encrypted connection. When using this option, your IP address and current location are not stored at any time. Please note that if you use a company-owned device, in particular a PC, it would be technically possible to trace your data there. Before finally submitting a report, you create a password and receive a personal case ID. The case ID and password give you access to your secure mailbox, allowing you to communicate with us in a protected manner while maintaining your anonymity.

The data you provide will be stored on a specially secured SpeakUp database on servers in the European Union. All data stored on the database is encrypted using state-of-the-art technology.

Recipients of personal data

We may share your personal data with authorities and other investigating bodies, in particular for the purpose of clarifying the facts and assessing the legal consequences.

Depending on the case, personal data from the SpeakUp system will be transferred to our affiliated companies in accordance with the principles described above.

In certain cases, we are obliged under data protection law to inform the person(s) named in your report of the allegations made against them. This is required by law, for example, if it is objectively clear that providing this information to these persons can no longer impair the investigation of the reported matter. If you have not submitted your report anonymously, we will not disclose your identity as a whistleblower – to the extent permitted by law – and will also ensure that no conclusions can be drawn about your identity. However, this may be possible based on the information you provide in your description of the facts. Please note that in the event of a knowingly false report with the intention of discrediting another person, we may be obliged to disclose your identity to that person.

In addition, your personal data may be disclosed to third parties (outside our company) in cases where this is necessary for the performance of the activity, for example to experts or external auditing companies for the purpose of conducting an audit.

Furthermore, IT service providers that we use to perform our tasks, in particular the operator of SpeakUp, may process your data. Here too, data is always transferred and processed for a specific purpose on the basis of an existing legal basis.

Transfer to third countries:

As a matter of principle, data is not transferred to third countries outside the EU, nor is this planned. If your personal data is transferred to third countries that the European Union has not determined to offer an adequate level of data protection, we use standard contractual clauses approved by the European Commission as an appropriate safeguard. In such cases, you can obtain a copy from our data protection officer.

Commission. In such cases, you can obtain a copy from our data protection officer.

If it is necessary and legally permissible to transfer your personal data to a court or authority in a non-European country without an adequate level of data protection in order to assert, exercise, or defend legal claims of our company, this may be done on the basis of Art.
49 (1) sentence 1 lit. e) GDPR without the need for additional measures to ensure an adequate level of data protection.

Information about your rights

With regard to your personal data, you have the following specific rights:

- Right to information about and access to your personal data,
- Right to request correction or deletion of your data
- Right to request restricted processing of your data or to object to it entirely
- Right to data portability,
- Right to lodge a complaint with the data protection supervisory authorities.

If the processing is based on your consent, you have the right to revoke this consent to the processing of the data at any time, in whole or in part, with effect for the future.

If the data processing is based on a balancing of legitimate interests, you have the right to object to this processing of the data. For this, there must be legitimate reasons arising from your particular situation.

Contact

If you have any questions regarding data protection or wish to exercise your rights, please contact the responsible body.

Data controller and data protection officer The operator of the whistleblower

system is responsible for data processing: **INDUS Holding AG**
Kölner Straße 32
D-51429 Bergisch Gladbach
Phone: +49 (0)2204/40 00-0
Email: indus@indus.de

The INDUS data protection officer can be contacted at:
fox-on Datenschutz GmbH
Pollerhofstr.
33a D-51789
Lindlar
Email: dsb+indus@fox-on.com

This privacy policy was created on September 9, 2025.