Data protection information on the Whistleblower System

We have set up a Whistleblower System to fulfill our legal obligations and to receive and clarify serious cases of suspected violations of rules within the Heidelberg Group.

Controller and Data Protection Officer

The Controller for the Whistleblower System is Heidelberger Druckmaschinen AG, Kurfürsten-Anlage 52-60, 69115 Heidelberg, Germany. The Data Protection Officer of Heidelberger Druckmaschinen AG can be contacted by mail at the above address with the addition of "Data Protection Officer" (please note in the first address line), via internal in-house mail, recipient "Data Protection Officer" (in a sealed envelope) or by e-mail: Datenschutzbeauftragter@heidelberg.com.

Anonymity and confidentiality

It is possible to submit a report via the Whistleblower System completely anonymously. The whistleblower's own personal data is entered into the Whistleblower System voluntarily. It is possible to submit a report without providing personal data. Incoming reports are always treated confidentially and are only accessible to a narrow circle of specially trained employees who are tasked with processing the reports.

In certain cases, we are legally obligated to inform the accused person about accusations that have been made. This may be the case, in particular, if it is objectively determined that providing information to this person cannot affect the clarification of the facts. However, the identity of the whistleblower or other information that could lead to conclusions about him or her will not be disclosed, insofar as this is legally permissible. We would like to point out that confidentiality cannot be guaranteed in the case of knowingly false information if the intention is to discredit individuals.

Purposes, data categories and legal basis of data processing

The following categories of data may be processed: name, address, gender, position in the company, personnel number, telephone number, access data, e-mail address, sound recordings, information about the reported matter and other information related to it, information about measures taken, IP address and other IT usage data.

In individual cases, special categories of personal data may also be processed. This may be the case if such are transmitted by the whistleblower or if their collection is necessary in the context of clarification measures. Such special categories of personal data will only be processed by us in accordance with the requirements of data protection law, in particular Art. 9 para. 2 GDPR or Section 26 para. 3 BDSG (Federal Data Protection Act).

We process personal data to fulfill our supervisory and compliance obligations pursuant to Art. 6 para. 1 lit. c GDPR.

To protect our overriding legitimate interest in averting damage and liability risks, we process personal data on the basis of Art. 6 para. 1 lit. f GDPR in conjunction with Sections 30, 130 OWiG (Administrative Offences Act).

Insofar as the processing is in connection with the fulfillment of foreign legal provisions to which we are subject, this is based on our overriding legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR.

Insofar as the processing is necessary for legal defense, this is also based on our overriding legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR.

If the processing is in connection with one of our employees, it is carried out in accordance with Section 26 para. 1 BDSG and serves to prevent criminal offenses or other violations.

If applicable, we also process personal data on the basis of an applicable company agreement for the establishment of a Whistleblower System pursuant to Section 26 para. 4 BDSG.

Data transfer

Categories of recipients of personal data

It may be necessary to pass on personal data to companies of the Heidelberg Group (e.g. if the whistleblowing relates to a matter of another Heidelberg company).

An external service provider based in the EU has been commissioned to provide the Whistleblowing System. A data processing agreement was concluded with this service provider in accordance with Art. 28 GDPR and the service provider processes the personal data exclusively in accordance with our instructions.

In addition, the disclosure of personal data in the context of clarification measures is possible in particular to the following (in individual cases also foreign) recipients: courts, authorities or other public bodies, external service providers, such as law firms or auditors, works councils or other stakeholders, insurance companies or opposing parties in the context of legal proceedings.

Data will only be passed on if this is necessary to fulfill the aforementioned purposes and if there are no interests worthy of protection that conflict with this.

Transfer to third countries or to an international organization

We will only transfer your data outside the European Economic Area (EEA) if the European Commission has confirmed an adequate level of protection for the third country or other appropriate data protection guarantees are in place, in particular by concluding EU standard contractual clauses with the recipient.

Storage period and origin of data

Storage period

With regard to the reports received, the following applies: Audio recordings are deleted 24 hours after confirmation of receipt. Connection data and log data are deleted after 2 days. Content data is deleted 14 days after the processing of the message has been completed.

Regarding the documentation of case files, the following applies: Personal data is stored for as long as it is required for case processing (clarification and evaluation) or due to legal requirements, or as long as we have a legitimate interest in storing it (for example, if it is required in the context of legal disputes). The duration of storage depends in particular on the severity of the suspicion and the effort required for processing.

From which sources your personal data originate

If we have not collected your personal data ourselves, we typically receive it from employees, business partners, other companies of the Heidelberg Group or courts, authorities or other bodies.

Necessity to provide personal data

You are not obliged to provide us with personal data.

Automated decisions, incl. profiling

No automated decisions are made in individual cases.

Right of access, rectification, erasure, restriction, data portability and objection

You as a data subject (as defined in Art. 4 No. 1 GDPR) are entitled to the rights listed below when your personal data is processed by us as a Controller (as defined in Art. 4 No. 7 GDPR).

Please address your requests to exercise your rights, your withdrawal or objection to the postal address listed under "Controller and Data Protection Officer" or send your message via the e-mail address listed there.

a) Data subject rights (Art. 15-20 GDPR)

You have the right of access (pursuant to Art. 15 GDPR), the right to rectification (pursuant to Art. 16 GDPR), the right to erasure (pursuant to Art. 17 GDPR), the right to restriction of processing (pursuant to Art. 18 GDPR) and the right to data portability (pursuant to Art. 20 GDPR) of your personal data if the legal requirements are met. Please note that there are legal restrictions on the right of access and the right to erasure (Sections 34, 35 BDSG).

b) Withdrawal of consent (Art. 7 para. 3 GDPR)

You may withdraw your declarations of consent under data protection law at any time. The withdrawal of your consent does not affect the lawfulness of the processing carried out on the basis of your consent until the withdrawal.

c) Individual right of objection (Art. 21 para. 1 GDPR)

If data processing is based on a legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR, you may object to this processing on grounds relating to your particular situation. We will then only continue to process the personal data if there are demonstrably compelling grounds for doing so that outweigh your interests, rights and freedoms, or if the processing serves to assert, exercise or defend legal claims.

d) Right to lodge a complaint (Art. 77 para. 1 GDPR)

You also have the right to lodge a complaint with a supervisory authority. The competent data protection supervisory authority for us is: "Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit", Königstraße 10 a, 70173 Stuttgart, poststelle@lfdi.bwl.de.