Data Protection module

Code of Conduct

Otto Krahn Group

In the interests of both data subjects and the company, we want to protect the confidentiality, integrity, availability, and authenticity of data throughout every stage of information processing.

In order to achieve this goal, we go beyond statutory regulations regarding the protection of personal data – we have also implemented appropriate technical and organizational measures. All Otto Krahn Group employees must be aware of the risks associated with the processing of personal data and take the necessary precautions to avoid such risks.

These guidelines represent a binding basis for the legally compliant and permanent protection of personal data in our company, as well as for protecting the personal rights of data subjects.

They are applicable to all Otto Krahn Group employees with regard to any interaction with personal data, whether in electronic or paper form. This includes data for all types of individuals (employees, customers, prospects, suppliers, service providers, etc.).

Definition of terms

Personal data means information referring to an identifiable natural person (hereinafter “data subject”). This includes information that makes it possible to identify that person, either directly or indirectly.

Special categories of personal data include data that permits the identification of a data subject's ethnicity, political opinions, religious or philosophical beliefs, or trade union membership.

They also include genetic data, biometric data that uniquely identifies a natural person, health data, or data concerning a natural person's sex life or sexual orientation.

Processors are natural or legal persons, authorities, institutions or other bodies commissioned by the Otto Krahn Group to process personal data. For better readability, this document does not explicitly refer to employees or other persons of (for example) "male" or "female" gender. References to persons are always addressed to all genders equally.

Data protection officer

The Otto Krahn Group has appointed an external data protection officer in accordance with the General Data Protection Regulation and the Federal Data Protection Act:

Felix Hudy
Managing Consultant on Data Protection
Attorney at Law
Phone: +49 40 790 235 - 278
E-Mail: fhudy@intersoft-consulting.de

Those of us who process personal data are trained and advised by the Data Protection Officer with regard to our obligations under GDPR and other data protection regulations. The data protection officer monitors compliance with the GDPR, other data protection-relevant regulations, and these guidelines and sensitizes employees to the subject of data protection.

Data subjects may contact the Data Protection Officer with questions about the processing of their personal data or the exercise of their associated rights. All inquiries will be treated confidentially. The Data Protection Officer is also responsible for communication with the supervisory data protection authority.

Principles of personal data processing

When processing personal data, we always observe the following principles: processing personal data always includes protecting it against unauthorized or improper use as well as accidental loss or destruction.

- Personal data is processed in a lawful manner, in good faith, and in a way that is comprehensible to the data subject.
- Personal data is only collected for legitimate, clearly defined purposes and is not additionally processed for any other purpose other than that for which it is intended.
- The scope of the personal data we collect is appropriate to its purpose and limited to the minimum necessary for processing.
- Personal data is factually correct and updated as necessary; we take all necessary measures to ensure that personal data found to be inaccurate for processing purposes is corrected or deleted without undue delay.
- Personal data is stored in a format that permits identification of data subjects only for as long as is necessary for the purposes of its processing.
- Appropriate technical and organizational measures are taken to ensure that personal data is processed in a manner that provides an adequate level of protection, including protection against unauthorized or improper use and accidental loss or destruction.

Special categories of personal data

In general, we only process special categories of personal data with the consent of the data subject or, in exceptional cases, with express legal permission. We protect special personal data by means of additional technical and organizational precautions (e.g. encryption during transmission, permissions restrictions).

Data processors

We are particularly careful when selecting service providers and suppliers who may have access to personal data. If this data is to be processed on behalf of the Otto Krahn Group, we ensure that the processorhas taken appropriate measures to ensure that all processing is carried out in accordance with the requirements of the GDPR and with regard to the protection of data subject rights.

When selecting service providers, besides considering their suitability with regard to competence in the actual processing of data, we also consider the technical and organizational security measures that the provider has implemented, as well as any aspects that can demonstrate the provider's reliability (data protection documentation, willingness to cooperate, response times, etc.).

We assess our data processors regularly with regard to any contractually agreed technical and organizational measures.

Data forwarding

Personal data may only be transferred to third parties with the legal approval or consent of the data subject. If therecipient of this personal data is located outside the European Union or the European Economic Community, we take special precautions to protect data subjects' rights and interests. We do not share data with recipients in countries that fail to provide an adequate level of data protection or other equivalent guarantees.

Data protection incidents

In the event that personal data protection is breached in any way (e.g. due to an IT-related incident or the loss of an unencrypted medium which results in unauthorized third-party access), we will submit a corresponding report to the supervisory data protection authority within 72 hours. In certain circumstances, the affected data subjects will also be notified of the breach.

Notification of supervisory bodies and/or data subjects is carried out in close consultation with the data protection officer.

Rights of data subjects

Data subjects have numerous rights in relation to the processing of their data. These include, for example, the right to transparency or information, the right to rectification of their personal data, and the right to withdraw or restrict their consent to the processing of this personal data. We support data subjects in exercising their rights.

Management shall take appropriate measures to provide data subjects with information in the most transparent, accessible, and comprehensible manner possible. If such revocation is justified, we will stop processing and storing the relevant data immediately.

Sensitization and training

All employees who are involved in processing personal data are sensitized to and trained on data protection to an appropriate extent and in a suitable manner.

Processing security

We work together with the processor to implement technical and organizational measures that ensure a level of protection appropriate to the level of risk. Numerous factors are taken into account here, including the current state of the art, the costs of implementation, and the nature, scope, circumstances, and purposes of data processing. We also take into account all risks to the rights and freedoms of natural persons and analyze the importance of these risks as well as the probability of their occurrence. These measures include, but are not limited to:

- Pseudonymization and encryption of personal data,
- The ability to restore availability of, and access to, personal data quickly following a physical or technical disruption,
- Procedures for the regular review, classification, and evaluation of the effectiveness of technical and organizational measures with a view to ensuring data processing security.

Use of Generative Artificial Intelligence

Inputting information into generative AI systems may result in this data being processed or stored by the provider. Therefore, the following principles apply:

- No input of personal data
- No input of confidential company information
- Compliance with international regulations
- When using services outside the EU, the respective local data protection regulations must be observed in addition to the GDPR.

Consequences of violations

Violating these guidelines or the data protection-related statutes may result in legal as well as employment-related consequences.

In the event of concrete and justified indications of a violation of one of the aforementioned principles, you are obliged to notify your direct manager, the Senior Director IT, the CFO or the Compliance function of the Otto Krahn Group. If you so desire, we will treat the information you provide as confidential to the extent permitted by law. You can also submit reports via our anonymous whistleblower system (https://otto-krahn-gruppe.integrityline.app/), which can also be accessed through our websites.

Otto Krahn Holding GmbH
Mühlenhagen 35, D-20539 Hamburg
www.ottokrahn.group

Otto Krahn Group

ALBIS

KRAHN

MOCOM

Otto Krahn New Business

KRAHN CERAMICS