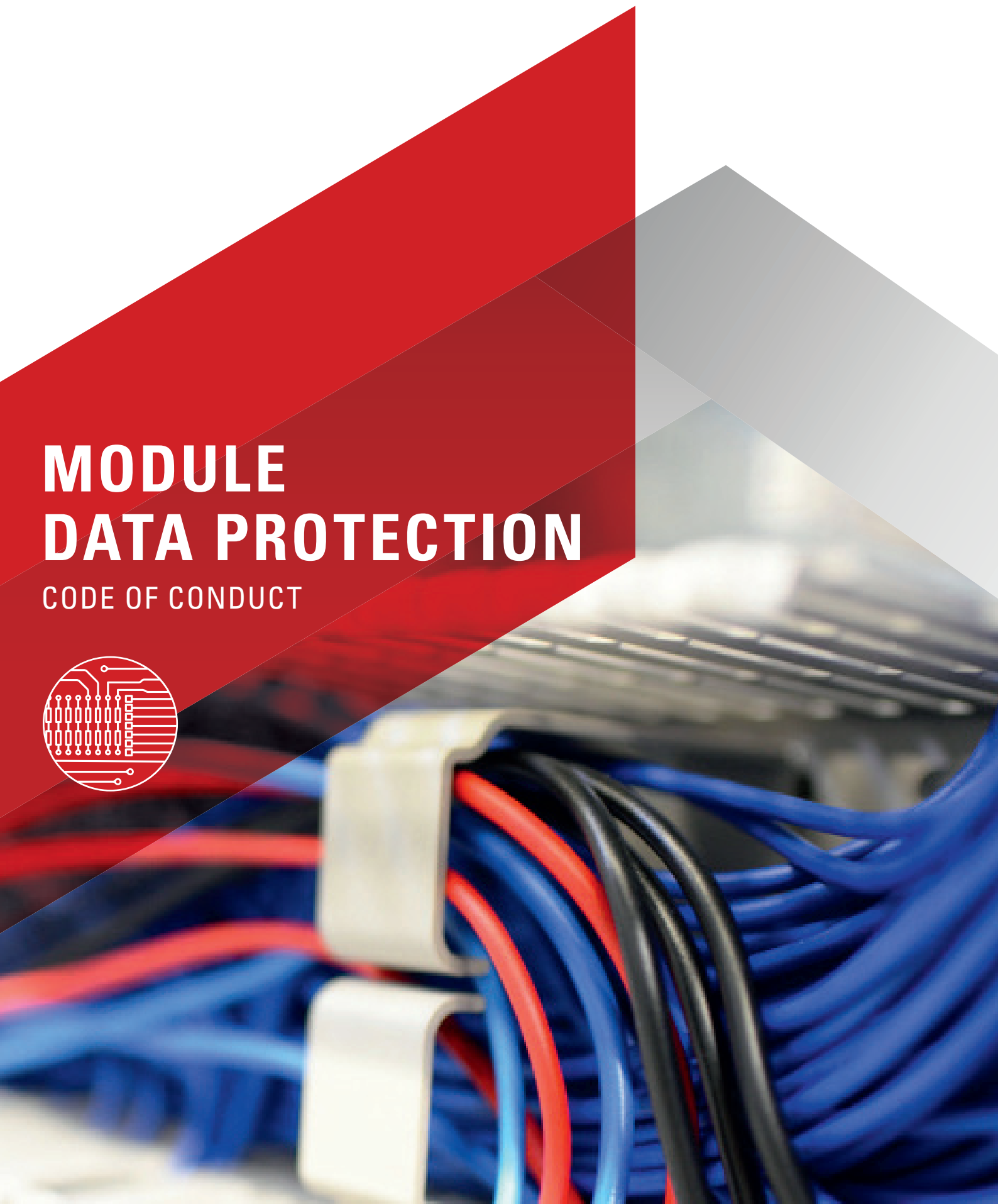
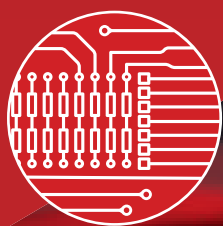


MODULE DATA PROTECTION

CODE OF CONDUCT



Preamble

In the interests of the affected persons 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 suitable technical and organizational measures. All OTTO KRAHN Group employees need to be aware of the risks associated with processing personal data, and must take the necessary precautions to prevent such risks.

These guidelines represent a binding basis for legally compliant and sustainable protection of personal data within our company, and for the protection and preservation of the personality rights of those affected.

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, interested parties, suppliers, service providers, etc.).

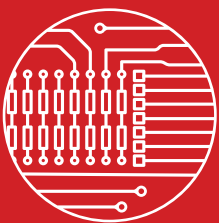
Definition of terms

Personal data means any information referring to an identifiable natural person (hereinafter “affected person”). This includes any information that might allow that person to be identified either directly or indirectly.

Special categories of personal data include information allowing identification of a person’s ethnicity, political opinions, religious or world views, or union membership status; it also includes genetic data, biometric information uniquely identifying a natural person, health information, or information on a natural person’s sex life or orientation.

Data processors are natural or legal persons, authorities, institutions, or other offices commissioned by the OTTO KRAHN Group to process personal data.

For readability purposes, this document does not specifically refer to (for example) “male” or “female” employees or other persons. All personal references are expressly intended to refer equally to persons of any gender.



Data protection incidents

In the event that personal data protection is violated for any reason (a breach resulting from an IT incident, for example, or the loss of an unencrypted medium leading to unauthorized third-party access) we will submit a report to the supervisory body for data protection within 72 hours. Under certain circumstances, the affected persons will also be notified of the breach. Notification of supervisory bodies and/or affected persons is carried out in close consultation with the data protection officer.

Rights of affected persons

Affected persons have a number of rights with regard to how their data is processed. These include, for example, the right to transparency or to information, the right to correct their personal data, or the right to withdraw or restrict their own consent to the usage of that personal data. We support affected persons in exercising their rights.

The executive management takes appropriate measures to convey information to affected persons in the most transparent, easily accessible, and comprehensible way possible. In the event of a justifiable objection, we will promptly stop processing and storing the data in question.

Sensitization and training

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

Processing security

We work with the data processor to take technical and organizational measures to ensure a level of protection appropriate to the degree of risk involved, taking numerous factors into consideration, including the current state of technology, the cost of implementation, and the type, scope, circumstances, and purposes of data processing. We also consider any risks to the rights and freedoms of natural persons, analyzing the severity of those risks as well as their likelihood of occurrence. Such measures include, among other things:

- ▶ Pseudonymization and encryption of personal data
- ▶ The ability to restore availability of, and access to, personal data quickly following a physical or technical disruption
- ▶ A procedure for regularly inspecting, rating, and evaluating the effectiveness of any technical and organizational measures in terms of ensuring data processing security

- ▶ Personal data is stored in a format that only permits identification of the affected persons for as long as is necessary to the purposes for which that data is being processed.
- ▶ Suitable technical and organizational measures are taken to ensure that personal data is processed in a way that includes an appropriate level of security; this includes protection against unauthorized or inappropriate use as well as unintentional loss or destruction.

Special categories of personal data

Generally speaking, we only process special categories of personal data with the affected person's consent or, in exceptional cases, with explicit permission to do so under the law. We also protect special personal data using additional technical and organizational precautions (e.g., encryption during transport, restrictions on authorizations).

Data processors

We are particularly cautious when selecting service providers and suppliers who may potentially have access to personal data. If this data is to be processed on behalf of the OTTO KRAHN Group, we ensure that the data processor has suitable measures in place to guarantee that all processing is done in accordance with the requirements of the GDPR and with a view to protecting the rights of the affected person(s).

When selecting service providers, in addition to considering their suitability in terms of competence regarding the actual processing of the data, we consider the technical and organizational security measures the service provider has in place, as well as any aspects that might shed light on the provider's reliability (data protection documentation, readiness to cooperate, reaction 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 forwarded to third parties with legal authorization or the consent of the affected person. We take special precautions to preserve the rights and interests of affected persons whenever the recipient of that personal data is outside the European Union or the European Economic Community. We do not forward data to recipients based in countries that lack an appropriate level of data protection or have other equivalent guarantees in place.

Data protection officer

In accordance with the General Data Protection Regulation and the German Data Protection Act, the OTTO KRAHN Group has appointed an external data protection officer:

Felix Hudy

Managing Consultant on Data Protection

Attorney at Law

Phone: +49 40 790235 – 278

E-Mail: fhudy@intersoft-consulting.de

The data protection officer teaches and advises those of us that process personal information on our obligations in accordance with the GDPR and other data protection-related regulations. He monitors compliance with the GDPR, other data protection-related regulations, and these guidelines, and sensitizes employees to the issue of personal data protection.

Affected persons can contact the data protection officer with any questions related to the processing of their personal information or exercising their rights in this context. All inquiries will be treated confidentially.

The data protection officer is also responsible for communicating with the supervisory body for data protection.

In addition to the data protection officer, you can also contact the Director of Human Resources at KRAHN Chemie on data protection-related questions; at ALBIS PLASTIC, you are welcome to contact the Senior Director of Information Technology.

Principles regarding processing personal data

Whenever we process personal data, we keep the following principles in mind:

- ▶ Personal data is processed in a lawful manner, in good faith, and in a way that is comprehensible to the affected person.
- ▶ Personal data is only collected for legitimate, clearly defined reasons, and does not undergo further processing for other unrelated reasons.
- ▶ The amount of personal data we collect is appropriate to its purpose, and is restricted to the minimum amount necessary for processing.
- ▶ Personal data is factually correct and updated as needed; we take all necessary measures to ensure that any personal data found to be incorrect for purposes of processing is immediately corrected or deleted.

Consequences of violations

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

Should you encounter concrete, reliable information regarding the violation of one of the aforementioned principles, you are obligated to notify your supervisor, the Tax & Legal Director and/or the CFO of the OTTO KRAHN Group. If you prefer, the information you share will be treated confidentially to the extent permitted by law. You can also make any notifications via our anonymous whistleblower system (**<https://www.bkms-system.com/ottokrahn>**) which can also be accessed through our websites.



ALBIS PLASTIC GmbH
Mühlenhagen 35, 20539 Hamburg
Tel. +49 40 78105-0
Fax +49 40 78105-361
info@albis.com
www.albis.com



KRAHN Chemie GmbH
Grimm 10, 20457 Hamburg
Tel. +49 40 32092-0
Fax +49 40 32092-322
info.de@krahn.eu
www.krahn.eu