



# DATA PROCESSING AGREEMENT (DPA)

KraLos GmbH – GDPR Data Processing Agreement for Businesses  
Version: Enterprise DPA v1.0 | Effective: May 2026

## 1. Parties to the Agreement

This Data Processing Agreement (“DPA”) is entered into between KraLos GmbH (“Data Processor”) and the respective customer (“Data Controller”).

This Agreement governs the processing of personal data in accordance with Article 28 of the GDPR.

## 2. Subject Matter of the Processing

KraLos processes personal data exclusively within the scope of the agreed SaaS, cybersecurity, and consulting services.

The processing may include, in particular:

- security analyses,
- log data,
- access data,
- threat detection,
- anomaly detection,
- network and security monitoring,
- incident response processes,
- technical support services.

## 3. Nature and Purpose of Processing

Processing is carried out exclusively for the purpose of:

- providing the services,
- ensuring system security,
- threat detection,
- attack detection,
- stability and performance monitoring,
- fulfilling contractual obligations.

## 4. Categories of personal data

Depending on the service, the following categories of data may be processed:

- User information,
- IP addresses,
- Log data,
- Authentication data,
- Technical device information,
- Communication data,
- Security-related event data.

## 5. Categories of Data Subjects

Data subjects may include, in particular:

- Employees,
- Customers,
- Service providers,
- Business partners,
- Users of the controller's systems.

## 6. Hosting & Infrastructure

KraLos's infrastructure is operated exclusively in Germany and within the European Union.

Hosting is provided by IONOS and affiliated European infrastructure providers.

Personal data is not transferred to non-EU countries unless a separate written agreement exists.

## 7. No Use of Google Analytics

KraLos does not use Google Analytics services.

To ensure security and stability, KraLos uses only its own data protection-oriented analysis, monitoring, and security mechanisms.

## 8. Technical and Organizational Measures (TOMs)

KraLos implements appropriate technical and organizational measures in accordance with Art. 32 of the GDPR.

These include, among others:

- Encryption,
- Access controls,
- Multi-factor authentication,
- Segmentation,
- Logging,
- Security monitoring,
- Access hardening,
- Digital twins,
- Adaptive protection mechanisms,
- Backup strategies,
- Role-based authorization systems,
- Incident response processes.

## 9. Confidentiality

KraLos requires all employees and subcontractors to maintain confidentiality and protect data.

Access to personal data is granted exclusively within the scope of the respective tasks and authorizations.

## 10. Subprocessors

KraLos is authorized to engage subprocessors.

These may include, in particular, hosting and infrastructure providers.

KraLos ensures that subprocessors guarantee an adequate level of data protection.

## 11. Obligations to Provide Support

KraLos supports the controller in the following matters:

- Data protection inquiries,
- Security incidents,
- Data breaches,
- Requests for information,
- Requests for erasure,
- Data protection impact assessments,
- Requests from authorities.

## 12. Reporting of Data Breaches

KraLos shall immediately inform the controller of any data breaches that come to light within KraLos's area of responsibility.

## 13. Rights of Inspection

The controller is entitled to request appropriate evidence of compliance with data protection requirements.

On-site audits require reasonable prior notice and must not unduly interfere with business operations.

## 14. Deletion and Return of Data

Upon termination of the contract, personal data will be deleted or returned in accordance with statutory retention obligations.

## 15. Liability

Liability is governed by the terms of the respective Master Service Agreement (MSA).

KraLos is not liable for data protection violations beyond KraLos's control.

## 16. Prohibited Use

Any misuse, manipulation, or unauthorized alteration of KraLos's systems or security mechanisms is prohibited.

Violations may result in:

- Account suspensions,
- Contract terminations,
- Claims for damages,
- Criminal prosecution.

## 17. Jurisdiction

German law applies.

The place of jurisdiction is Hanover, Germany.