UNIKRON PRIVACY POLICY

Last Updated: 29.10.2025

Controller: Nokor GmbH, Haltenweg 4, 8832 Wilen, Switzerland ("Nokor," "We," "Us").
Applicable Law: This policy is based on the Swiss Federal Act on Data Protection (FADP/DSG) and, where applicable, the EU General Data Protection Regulation (GDPR).

1. PRINCIPLES AND CONTACT

We process Personal Data lawfully, in good faith, and on a proportional basis, limiting processing to the purpose disclosed herein. All data processing activities are conducted in accordance with our contractual obligations under the UNIKRON Master Terms of Service.

Data Protection Contact:
Nokor GmbH
Attn: Data Protection Officer
Email: compliance@unikron.ch

2. DATA COLLECTION, PURPOSE, AND LEGAL BASIS

We collect and process Personal Data primarily for two categories of data subjects: our Institutional Client Contacts and the End-Users whose data is passed to us by our Clients.

Data Subject Category	Data Examples	Purpose of Processing	Legal Basis (FADP/GDPR)
Institutional Contacts (Client employees, signatories, compliance contacts)	Name, Email, Title, Phone, IP address for login, KYC/AML documentation.	To fulfill the contract (Master ToS, ICA); Account management; Billing; Regulatory compliance checks (KYC/AML); Security monitoring; Fraud prevention.	Contract performance; Legitimate interest (Security, Fraud prevention, business operations); Legal obligation (AML/KYC).
End-Users (via Client APIs)	User IDs, API Call Parameters,	To provide the Services as a data processor on	Performance of our contract with the Client

	Transaction Hashes, Wallet Addresses, Usage Logs, Device Information.	behalf of the Client (Controller); Infrastructure maintenance; Security incident response; System optimization; Fraud and abuse prevention.	(the Controller); Legitimate interest (Security, Fraud prevention, infrastructure maintenance, system integrity).

3. DISCLOSURE OF DATA AND CROSS-BORDER TRANSFERS

We do not sell Personal Data. We disclose data only as necessary to provide the Services, protect our legal rights, or comply with the law.

Recipients: We use selected sub-processors (e.g., cloud hosting providers, security monitoring services, internal IT systems) to process data. These processors are contractually bound by the Data Processing Agreement (DPA) to protect data at the same standard as outlined in this policy.

International Transfers: As a global technology infrastructure provider, Personal Data may be transferred to and processed in countries outside of Switzerland. Our primary data processing occurs in the United States (US), using infrastructure provided by major cloud providers. We ensure that any such transfer is governed by appropriate safeguards in accordance with the FADP and the GDPR, where applicable. These safeguards include transferring data to countries deemed to provide an adequate level of protection, or by implementing the European Commission's Standard Contractual Clauses (SCCs) supplemented by additional technical and organizational measures.

A current list of sub-processors and specific data processing locations is available to Clients upon request to compliance@unikron.ch.

4. DATA RETENTION

We store Personal Data only for the duration necessary to fulfill the purposes set out in this policy or as required by mandatory retention periods.

- **Client Account Data:** Retained for the duration of the contractual relationship plus 10 years following termination to comply with Swiss commercial and tax law obligations.

Data deletion after the retention period may be subject to manual review and processing.

- **Technical Logs and API Data:** Retained for a period of 12 months for security, debugging, and service improvement purposes. **Deletion of expired data is performed on a periodic basis and may not be immediate upon expiration.**
- **KYC/AML Documentation:** Retained for 10 years following the end of the business relationship as required by Swiss anti-money laundering regulations. **Such documentation may be retained longer if required by ongoing legal or regulatory obligations.**

5. YOUR RIGHTS

Under FADP and GDPR (where applicable), data subjects have the following rights:

Right to Information (Auskunftsrecht): The right to know whether we process your data and, if so, which data, the purpose, and the recipients.

Right to Correction (Berichtigung): The right to have inaccurate or incomplete data corrected.

Right to Deletion (Löschung): The right to request the deletion of your data, provided there is no overriding legal reason or legitimate interest for its continued retention.

Right to Object (Widerspruchsrecht): The right to object to the processing of your data based on legitimate interests.

Right to Data Portability: Where applicable, the right to receive your data in a structured, commonly used format.

To exercise these rights, please contact us at compliance@unikron.ch. We will respond to your request within 30 days. We reserve the right to verify your identity before processing any data subject request and may charge a reasonable fee for manifestly unfounded or excessive requests.

Data Subject Access Requests, Data Deletion Requests, and Data Portability Requests will be processed manually upon receipt of a verified request. Data exports will be provided in commonly used electronic formats (JSON, CSV, or PDF) as appropriate for the data type. Deletion requests will be subject to our legal retention obligations and may result in anonymization rather than complete deletion where legal retention is required.

6. DATA SECURITY

We implement comprehensive Technical and Organizational Measures to ensure a level of security appropriate to the risk, in accordance with Article 8.3 of the Master ToS. These measures include, but are not limited to:

- Encryption of data in transit (TLS 1.3) and at rest (AES-256)
- Secure authentication protocols commensurate with service tier and risk assessment
- Internal vulnerability scanning and security reviews
- Infrastructure and internal controls designed based on industry-standard security frameworks (e.g., SOC 2)

7. POLICY UPDATES AND DISPUTE RESOLUTION

7.1 Integration with Legal Framework

This Privacy Policy is an integral part of UNIKRON's legal framework and forms a binding part of the agreement between you and Nokor GmbH. It should be read in conjunction with our Master Terms of Service, Institutional Client Addendum, and Data Processing Agreement, which together constitute the complete contractual relationship.

7.2 Policy Updates

We may update this Privacy Policy from time to time. We will provide notice of any material changes through our Services or via email. Continued use of our Services after such changes constitutes acceptance of the updated policy.

7.3 Governing Law and Jurisdiction

This Privacy Policy and any disputes related to it shall be governed by Swiss law, and the exclusive place of jurisdiction shall be Schwyz, Switzerland, as specified in Article 12 of the Master Terms of Service.