Information Security Policy

Organisation: tolinax UG (haftungsbeschränkt), Oberhof 4, 83700 Oberhof, Germany — operator of the aYOUne business platform Status: Approved by the Managing Director and published. Version 1.0, effective 2026-10-14 Owner: Managing Director (Maximilian Hanrieder) Review cycle: at least annually, after major incidents and after significant changes to the platform

1. Purpose

This policy sets out how tolinax protects the confidentiality, integrity and availability of the aYOUne platform and of the data that customers (tenants) and their end customers entrust to it. It is the umbrella document of the information security programme; the sub-policies listed in section 6 contain the details.

2. Scope

All systems, services, source code, infrastructure, devices and people (employees, contractors, automated agents) involved in developing and operating aYOUne.

3. Security objectives

- Strict separation of customer data between tenants.
- Access to personal data only for authorised persons with a business need (least privilege).
- Encryption of data in transit and protection of secrets at rest.
- Early detection of and fast response to security incidents.
- Continuous identification and remediation of vulnerabilities.
- Compliance with the GDPR and the German Federal Data Protection Act (BDSG).

4. Implemented technical controls (summary)

| Area | Control | |---|---| | Hosting | Google Kubernetes Engine and MongoDB Atlas in the Google Cloud region europe-west3 (Frankfurt, Germany); object storage in europe-west3 | | Tenant isolation | Every record carries a tenant identifier; the shared data-access layer scopes queries to the authenticated user's tenant | | Authentication | Central authentication service; passwords hashed with bcrypt; second factor via TOTP, YubiKey or WebAuthn/passkeys; account lockout after repeated failed attempts; rate limits on login and second-factor endpoints | | Sessions | Short-lived access tokens (15 minutes) with rotating, tracked refresh tokens | | Authorisation | Role-based access control with fine-grained rights per entity and action, enforced on every API route; customer package rights additionally restrict what a tenant may use | | Transport security | HTTPS only (HTTP redirected to HTTPS) at the public gateway with publicly trusted certificates; HSTS (1 year, including subdomains) | | Secrets | Third-party credentials stored encrypted in a credential vault (AES-256-GCM; optional end-to-end mode where the server cannot decrypt) | | Network | Ingress only through a managed service-mesh gateway; internal metrics endpoints blocked from the internet; IP block lists for abusive sources; workload separation via dedicated node pools | | Monitoring | Prometheus/Alertmanager alerting, dashboards, automatic capture of runtime errors as tracked tasks, public status page | | Audit trail | Authentication events and API actions logged with user and tenant context | | Vulnerability management | Recurring security audits with tracked findings and re-verification |

5. Organisational controls

- Security responsibilities are held by the Managing Director, who approves this policy and its sub-policies.
- Staff and contractors are bound to confidentiality and to the Internal Data Protection Policy.
- Access rights are granted on a need-to-know basis and removed when no longer needed.
- Workplace baseline, in force on all company devices and consoles: active anti-malware protection with automatic updates, automatic screen lock, unique strong passwords stored in a password manager, multi-factor authentication on all company, cloud, source-control and database-console accounts, clear-desk and clear-screen practice, no company data on unmanaged storage, current operating system and security updates.
- Security incidents are handled according to the Incident Response Policy.
- Suppliers that process personal data are selected with regard to data protection and are bound by data processing terms (for the large infrastructure providers such as Google Cloud and MongoDB Atlas: the providers' standard data processing addenda).

6. Sub-policies

Access Control Policy

Data Classification and Encryption Policy

Network Security and Monitoring Policy

Incident Response Policy

Vulnerability Management Policy

Data Retention and Deletion Policy

Internal Data Protection Policy

7. Compliance and exceptions

Exceptions to this policy require written approval by the Managing Director, a documented risk assessment and an expiry date. Violations may lead to disciplinary or contractual consequences.

8. Publication

This policy and its sub-policies are published on the aYOUne trust page: https://ayoune.com/en/trust (German: https://ayoune.com/de/trust).

Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-10-22 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: info@tolinax.com