Data Classification and Encryption Policy

Organisation: tolinax UG (haftungsbeschränkt), operator of the aYOUne platform Status: Approved by the Managing Director and published. Version 1.0, effective 2026-10-14 Owner: Managing Director Review cycle: at least annually

1. Classification levels

| Level | Description | Examples | |---|---|---| | Public | Intended for publication | Marketing pages, public documentation | | Internal | Business information without personal data | Product configuration, non-personal statistics | | Confidential | Customer business data and ordinary personal data | Contacts, orders, invoices, employee records | | Strictly confidential | Credentials, authentication factors, payment data, special categories of personal data (Art. 9 GDPR, e.g. biometric voice or face data) | Passwords, second-factor secrets, API keys, OAuth tokens, voice samples |

All customer (tenant) data is treated as at least Confidential.

2. Classification in the platform (implemented)

- The platform's central data catalogue marks entities with a personal-data level (none, low, high); this marking drives data-protection tooling such as exports and erasure planning. Coverage of the catalogue is being extended to all entities.
- Password hashes and other secret fields are excluded from default query results.
- Request data that is passed to error reporting is reduced to an allow-list of fields, and secrets in query strings are redacted.

3. Encryption in transit (implemented)

- All public endpoints are served over HTTPS (TLS) at the service-mesh gateway; HTTP requests are redirected to HTTPS; certificates are issued by a public certificate authority and renewed automatically.
- HTTP Strict Transport Security with a one-year max-age including subdomains.
- Connections to the managed database service use TLS.
- Webhooks from payment and other providers are verified with the providers' signatures.

4. Encryption at rest (implemented)

- The database (MongoDB Atlas) and object storage (Google Cloud Storage) are hosted in Frankfurt, Germany, and encrypt all stored data and backups at rest by default (provider-managed AES-256).
- Third-party credentials of tenants are additionally encrypted at application level with AES-256-GCM before storage. An optional end-to-end mode derives the key on the client (PBKDF2-SHA256, 600,000 iterations, AES-256-GCM) so that the server cannot decrypt the secret.
- Passwords are stored only as bcrypt hashes.
- Data exports for data subjects are stored encrypted and delivered via time-limited signed links.

5. Handling rules

- Strictly confidential data must never be written to logs, tickets, chat messages or e-mails in clear text.
- Confidential data may only be shared with sub-processors under data processing terms (individual agreements or the provider's standard data processing addendum).
- Test and demonstration use only test data.

6. Planned improvements

- Extend the personal-data marking to all entities of the data catalogue.
- Migrate remaining older credential records to the current AES-256-GCM format.
- Enforce mutual TLS for internal service-to-service traffic (planned; not yet enforced).

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