

Security & Privacy

Information security and data protection policies of tolinax UG (haftungsbeschränkt) for the aYOUne platform.

8 Seiten in dieser Sammlung.

Access Control Policy

Access Control 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; access reviews at least every six months

1. Principles

- Least privilege: every person and service receives only the rights required for its task.
- Need to know: personal data is accessible only to those who need it to perform the service.
- Separation of tenants: users of one customer can never access another customer's data, unless an explicit, documented relationship exists (for example an agency managing a client account) and the user has been granted access to that account.

2. Platform access control (implemented)

Authentication through the central authentication service. Passwords are hashed with bcrypt and must be at least 8 characters long. Users can enable a second factor (TOTP authenticator app, YubiKey or WebAuthn/passkey). Repeated failed login or second-factor attempts lock the account temporarily; login and second-factor endpoints are rate-limited.

Tokens: access tokens expire after 15 minutes; refresh tokens are rotated and tracked individually so they can be revoked.

Role-based authorisation: rights follow the scheme <entity>.<action> (view, create, edit, delete, export, import and specific actions). Every API route declares the rights it requires and the request is rejected if the user lacks them. A user's effective rights are the intersection of the rights of the user's role and the modules licensed by the customer.

Tenant isolation: every stored record carries the owning tenant identifier; the shared data-access layer limits all reads and writes to the authenticated user's tenant.

Record-level restriction: individual records can be restricted to named users or teams.

Operator (superuser) access: platform-wide administrative functions are limited to a separate superuser account type with its own rights catalogue and token revocation.

API keys and integrations: API keys are scoped per tenant; third-party credentials are kept in the encrypted credential vault.

Logging: authentication events and API actions are logged with user, tenant, IP address and timestamp.

3. Internal access to production (organisational)

- Access to the cloud console, Kubernetes cluster, database and source code repositories is limited to named individuals and protected with multi-factor authentication (enforced on all such accounts).
- Production database access for staff is read-only by default; changes go through the platform's APIs or reviewed migration tooling.
- Access is revoked immediately when a person leaves or changes role.
- Access rights are reviewed at least every six months.

4. Planned improvements

- Stronger password rules (longer minimum length, check against known breached passwords).
 - Mandatory second factor for all administrator accounts of customers.
 - Further per-service scoping of infrastructure secrets.
-

Data Classification and Encryption Policy

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).

Data Retention and Deletion Policy

Data Retention and Deletion 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. Principles

- Personal data is kept only as long as needed for the purpose it was collected for, or as long as a legal retention obligation applies (for example German commercial and tax law, §§ 147 AO, 257 HGB).
- Customers (tenants) are the controllers of the data they process in aYOUne; tolinax deletes or returns that data on their instruction.

- Where a legal retention obligation prevents deletion, the data is restricted (blocked from further processing) and pseudonymised instead of deleted, and deleted once the obligation ends.

2. Data subject requests (implemented controls)

- Erasure (Art. 17 GDPR): the platform provides an erasure workflow for end-customer records (consumers). It first produces a plan (dry run) listing every affected record, then executes on explicit confirmation by an authorised user holding dedicated rights. Records are deleted, unlinked from related records, or — where a retention obligation applies — pseudonymised and blocked. Every run is written to an audit log.
- Access and portability (Art. 15 / 20 GDPR): the platform generates a data export for a data subject as an asynchronous job. The result is stored encrypted and made available through a time-limited signed download link; exports are removed after 30 days by default.
- Requests are answered within one month (Art. 12(3) GDPR).

3. Backups

- Tenant backups can be created on request and on a schedule; scheduled backups are pruned according to a per-tenant retention rule.
- Deleted data may persist in backups until those backups expire under the backup retention period. Backups are not restored into production except for disaster recovery, and any data deleted earlier is deleted again after a restore.

4. End of contract

On termination of a customer contract, tolinax:

- offers the customer an export of its data;
- deletes the customer's tenant data from the production systems within 30 days after contract end, unless a legal obligation requires retention;
- lets the remaining copies in backups expire within the backup retention period.

Current implementation status: strong (second-factor) confirmation for tenant deletion is implemented; the automated tenant archive-and-delete workflow is in development. Until it is available, tenant deletion at contract end is carried out as a documented manual operation by the operator.

5. Logs

Application and audit logs are retained for operational and security purposes. Request data passed to error reporting is reduced to an allow-list of fields with query secrets redacted. Logs are kept only as long as needed for operation and security and are then deleted.

Incident Response Policy

Incident Response 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 (Geschäftsführer) Review cycle: at least annually and after every major incident

1. Purpose and scope

This policy defines how tolinax detects, handles, documents and reports security incidents and personal data breaches affecting the aYOUne platform, its infrastructure and the data processed on behalf of customers (tenants).

A security incident is any event that compromises or threatens the confidentiality, integrity or availability of systems or data. A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art. 4(12) GDPR).

2. Roles

| Role | Responsibility | |---|---| | Incident Owner (Managing Director) | Final decisions, external notifications (supervisory authority, customers, partners), approval of closure | | Incident Handler (on-duty engineer) | Triage, containment, technical investigation, evidence preservation | | Communications | Status page updates and customer communication, approved by the Incident Owner | | Privacy contact | Assessment of whether personal data is affected and whether Art. 33/34 GDPR notifications are required |

In a small organisation one person may hold several roles; the Incident Owner role is never delegated for external breach notifications.

3. Detection (implemented controls)

- Runtime errors of every service are persisted automatically as tracked tasks of type "Bug" ("errors as tasks"), so that no failure is silently lost.
- Platform services expose health and readiness endpoints; Kubernetes restarts unhealthy workloads and failures are visible in the operations tooling.
- A public status page (status.ayoune.app) with component monitoring and an incident workflow is used to publish incidents and their resolution.
- Authentication events (logins, failed attempts, second-factor events) and API actions are logged with tenant and user context.
- Periodic security audits with tracked findings and re-verification (see Vulnerability Management Policy).

4. Response process

Report — anyone (employee, contractor, customer, researcher) reports a suspected incident to the security contact. Internal reports go directly to the Incident Owner.

Triage (target: within 4 hours of detection) — classify severity (Critical / High / Medium / Low) and determine whether personal data may be affected.

Contain — revoke or rotate affected credentials and tokens, block abusive sources, disable or roll back affected deployments.

Investigate — preserve logs and evidence, establish the root cause, affected tenants, data

categories and number of data subjects.

Eradicate and recover — deploy the fix, verify it, restore from backup where needed.

Notify — see section 5.

Post-incident review — written root-cause analysis with corrective actions tracked as tasks until closed.

5. Notification of personal data breaches

- Customers (tolinax as processor): affected customers are informed without undue delay, and in any case within 48 hours after tolinax becomes aware of a breach affecting their data, including the nature of the breach, data categories, approximate number of data subjects, likely consequences and measures taken. Follow-up information is provided as it becomes available.
- Platform partners / marketplaces: where a breach affects data received from a sales channel or partner (for example a marketplace integration), the partner is notified within the timeframe required by the partner agreement, and no later than the customer notification above.
- Supervisory authority (tolinax as controller): within 72 hours after becoming aware (Art. 33 GDPR), unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Data subjects: without undue delay where the breach is likely to result in a high risk (Art. 34 GDPR).
- Every breach, including those not notified, is documented in a breach register with facts, effects and remedial action (Art. 33(5) GDPR).

6. Contact

Security reports: security@ayoune.com (also published in `/.well-known/security.txt`). Privacy reports: privacy@tolinax.com.

7. Breach register

All security incidents and personal data breaches are recorded in a breach register maintained by the Incident Owner (facts, effects, remedial action, notifications made or the reason for not notifying).

Information Security Policy

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>).

Internal Data Protection Policy

Internal Data Protection 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, and whenever processing activities, sub-processors or legal requirements change. Each review is recorded with date and reviewer.

1. Scope and roles

This policy applies to all employees, contractors and automated agents acting for tolinax. tolinax acts as:

- Controller for its own business data (customers' contact persons, website visitors, applicants, employees);
- Processor for the personal data that customers (tenants) process in the aYOUne platform, acting only on their documented instructions under a data processing agreement (Art. 28 GDPR).

2. Principles (Art. 5 GDPR)

Lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

3. Rules for staff

Process personal data only as needed for the assigned task and only through the platform's access-controlled interfaces.

Never copy production personal data to private devices, private accounts or unapproved tools.

Use test tenants and test data for tests and demonstrations; never use real customer names in public texts or examples.

Do not share credentials; use the platform's credential vault for third-party secrets.

Report any suspected data breach immediately to the Managing Director (see Incident Response Policy).

Confidentiality obligations apply to all staff and continue after the end of employment.

4. Sub-processors

Personal data is passed to sub-processors (hosting, database, e-mail delivery, payment, AI providers and others) only under data processing terms — for the large providers (for example Google Cloud and MongoDB Atlas) these are the providers' standard data processing addenda; tolinax has not negotiated individual agreements with them — and, for transfers outside the EU/EEA, with an appropriate transfer mechanism (EU-U.S. Data Privacy Framework or the EU Standard Contractual Clauses 2021). The current list of sub-processors is published on the trust page (<https://ayoune.com/en/trust>).

5. Data subject rights

Requests for access, rectification, erasure, restriction, portability and objection are handled within one month. The platform provides tooling for data export and erasure (see Data Retention and Deletion Policy). Where tolinax is processor, requests are forwarded to the responsible customer without delay and tolinax supports the customer in answering them.

6. Records and accountability

- A record of processing activities (Art. 30 GDPR) is maintained.
- Technical and organisational measures (Art. 32 GDPR) are documented in the Information Security Policy and its sub-policies.
- Data protection impact assessments are carried out for high-risk processing (for example biometric voice or video data).

7. Contact

Privacy contact: privacy@tolinax.com. tolinax has not appointed a Data Protection Officer because the statutory requirements for an appointment (Art. 37 GDPR, § 38 BDSG) are not met; privacy matters are the responsibility of the Managing Director.

Network Security and Monitoring Policy

Network Security and Monitoring 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. Architecture (implemented)

- Production runs on Google Kubernetes Engine in europe-west3 (Frankfurt, Germany). The database is a managed MongoDB Atlas cluster in the same region.
- All inbound internet traffic enters through a single service-mesh ingress gateway (Istio). Services are not exposed individually to the internet; only explicitly routed hostnames are reachable.
- Workload classes are separated: crawler workloads run on a dedicated, tainted node pool, isolated from API and worker workloads.
- Real-time media and remote-support relays that need raw TCP/UDP run in their own namespaces behind dedicated load balancers.
- Build and package infrastructure (private package registry, CI runners) is hosted separately at Hetzner in Nuremberg, Germany, and holds no customer data.

2. Protective controls (implemented)

- HTTPS-only public endpoints; HTTP is redirected.
- Internal metrics endpoints are blocked at the gateway for external requests.
- IP block lists at the gateway for abusive sources.
- Rate limiting on all APIs (Redis-backed) with stricter limits on login, second-factor, verification and PIN endpoints; account lockout after repeated failures.
- Security headers on API responses (including HSTS).
- Inbound webhooks are accepted only with valid provider signatures.

3. Monitoring and detection (implemented)

- Prometheus with Alertmanager collects metrics from the cluster and services; alerts are delivered to the operations team in real time via a messaging channel.
- Dashboards for service health and resource usage.
- Kubernetes health and readiness probes restart unhealthy services automatically.
- Runtime errors of every service are recorded automatically as tracked bug tasks.
- Authentication events and API actions are logged centrally.
- A public status page reports component status and incidents.

4. Planned improvements

- Kubernetes network policies (default-deny between namespaces and workloads).
- Strict mutual TLS inside the service mesh with authorisation policies (internal traffic is not yet

mutually authenticated).

- Evaluation of a web application firewall in front of the ingress gateway.
-

Vulnerability Management Policy

Vulnerability Management 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. Sources of vulnerability information

- Internal security audits of the code base and infrastructure (a comprehensive audit was carried out in May 2026, with findings tracked and re-verified in June and August 2026).
- Reports from researchers and customers through the security contact published in /security.txt (security@ayoune.com).
- Security advisories of the frameworks, libraries, cloud and SaaS providers in use.
- Runtime error monitoring (errors are captured automatically as tracked tasks).

2. Process

Record every finding as a tracked task with severity (Critical, High, Medium, Low).

Assess exploitability and affected data.

Remediate within these target times:

| Severity | Target time to fix or mitigate | |---|---| | Critical | 7 days | | High | 30 days | | Medium | 90 days | | Low | next planned release / risk-accepted |

Verify the fix (re-test of the finding against the deployed code) before closing.

Accept risk only with a written decision by the Managing Director, recorded with a reason and review date.

3. Patch management

- All services are built as container images from shared base images and redeployed through automated pipelines; shared platform libraries are released centrally and pulled into services through a controlled version-bump process.
- Managed services (Kubernetes control plane, database) receive provider security updates.

4. Planned improvements

- Automated dependency and container-image scanning in the build pipelines.
 - An external penetration test.
-

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