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).

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