TOMs ALAI AI Services v1

Technical and Organizational Measures (TOMs)

ALAI Holding AS — AI Services

Version: 1.0 | **Date:** 2026-05-01 | **GDPR Reference:** Article 32

Overview

This document describes the technical and organizational measures (TOMs) implemented by **ALAI Holding AS** to ensure the security of personal data processed on behalf of clients in connection with AI Services.

ALAI acts as a **Data Processor** when delivering AI services (AI audits, AI development, AI agent orchestration) to clients. This document satisfies GDPR Article 28(3)(c) requirement to demonstrate appropriate security measures.

Technical Measures

2.1 Encryption

Measure	Implementation	Purpose
Data in Transit	TLS 1.3 for all HTTP connections; SSH for server access	Protect data during transmission
Data at Rest	AES-256 encryption for PostgreSQL databases, file storage, and backups	Prevent unauthorized access to stored data
API Keys and Secrets	Stored in Bitwarden (encrypted vault); environment variables in production; never committed to git	Protect credentials

Measure	Implementation	Purpose
Email	TLS for SMTP/IMAP; PGP available for sensitive communications	Secure email in transit

Implementation Details:

- All client-facing web services enforce HTTPS via Cloudflare SSL
- Database connections use SSL/TLS (Azure PostgreSQL enforces encrypted connections)
- Backups encrypted at rest using Azure Storage encryption (Microsoft-managed keys)

2.2 Pseudonymization

Measure	Implementation	Purpose
Development/Test Data	Client production data is anonymized before use in dev/test environments	Minimize exposure of real personal data
Logging	Personal identifiers (emails, names) are redacted or hashed in system logs	Prevent leakage via logs
AI Training Data	Client data used for AI model fine-tuning is pseudonymized where feasible	Protect individual identities in training datasets

2.3 Access Control

Measure	Implementation	Purpose
Multi-Factor Authentication (MFA)	Required for all production system access (Azure Portal, SSH, Bitwarden, Documenso, BookStack admin)	Prevent unauthorized access
Role-Based Access Control (RBAC)	Azure AD roles limit production access to designated personnel only	Need-to-know principle
SSH Key Authentication	Password authentication disabled; only SSH keys allowed for server access	Prevent brute-force attacks
API Token Rotation	Quarterly rotation of service API tokens	Limit token exposure window

2.4 Logging and Monitoring

- **Audit Logs:** All access to production databases and personal data logged with timestamps, user ID, action
- **Retention:** Logs retained for 90 days (compliance requirement)
- **Alerting:** Failed login attempts, unauthorized access attempts trigger alerts to CEO

- **Review:** Monthly log review for anomalies

2.5 Security Updates

- **Patch Cycle:** Monthly security updates for OS and dependencies
- **Dependency Scanning:** Automated vulnerability scanning via Dependabot (GitHub) and npm audit
- **Critical Patches:** Applied within 48 hours of disclosure for high-severity vulnerabilities

2.6 Penetration Testing

- **Frequency:** Annual external penetration testing (planned Q4 2026)
- **Scope:** Web applications, API endpoints, authentication mechanisms
- **Remediation:** High/critical findings remediated within 30 days

Organizational Measures

3.1 Personnel Security

Measure	Implementation	Purpose
GDPR Training	Annual GDPR training for all staff with data access	Ensure awareness of data protection obligations
Confidentiality Agreements	All employees and contractors sign NDAs covering client data	Legally binding confidentiality
Background Checks	Reference checks for all hires with production access (Norway/Bosnia)	Vet trustworthiness
Access Termination	All access revoked within 24 hours of employee/contractor departure	Prevent ex-employee access

3.2 Access Management

- **Need-to-Know Principle:** Access granted only when documented business need exists
- **Access Review:** Quarterly review of who has production access; revoke unnecessary permissions
- **Temporary Access:** Time-limited credentials for contractors (expire after engagement)

3.3 Backup and Recovery

Measure	Implementation	Target
Backup Frequency	Daily automated backups of all databases	RPO: 24 hours (max data loss)
Backup Location	Azure Blob Storage (geo-redundant, EU region)	Survive regional outage
Recovery Time	Tested quarterly restore procedures	RTO: <24 hours (time to restore)
Backup Encryption	AES-256 encryption at rest	Protect backup data

3.4 Incident Response

Data Breach Response Plan:

1. **Detection:** Automated alerts + manual log review
2. **Containment:** Immediate isolation of affected systems (within 1 hour)
3. **Assessment:** Determine scope: what data, how many records, what breach type
4. **Notification:**
   - Client notification within **24 hours** of breach discovery (per DPA)
   - Datatilsynet (Norwegian DPA) notification within 72 hours if required by GDPR
5. **Remediation:** Patch vulnerability, restore from backup if needed
6. **Documentation:** Full incident report with timeline, root cause, remediation steps

Incident Contact: alem@alai.no (CEO, available 24/7 for critical incidents)

3.5 Data Retention and Deletion

Data Type	Retention Period	Deletion Method
Client personal data (production)	Duration of contract + 30 days post-termination	Secure deletion (multi-pass overwrite or Azure storage deletion)
Backups	90 days rolling window	Automatic expiry
Audit logs	90 days	Automatic expiry
Signed contracts (NDA, Retainer, DPA)	7 years (Norwegian accounting law)	Archived at archive.alai.no per ZAKON ARCHIVE FIRST

Data Deletion Verification: Upon contract termination, ALAI provides written confirmation of data deletion within 30 days (per DPA section 3.7).

Sub-Processor Security

ALAI relies on sub-processors for infrastructure and AI services. Each sub-processor has been vetted for GDPR compliance:

Sub-Processor	Certifications	Data Location
Anthropic PBC	SOC 2 Type II, GDPR DPA, SCCs	USA (AWS us-east-1)
Microsoft Azure	ISO 27001, SOC 2, GDPR compliant	EU West / Norway East
Cloudflare Inc.	ISO 27001, SOC 2 Type II, GDPR DPA	Global (EU data residency)
Brevo	GDPR compliant, ISO 27001	EU (Frankfurt)

See DPA Template for full sub-processor details and 30-day notice policy.

Compliance and Audit

- **Annual TOMs Review:** CEO reviews and updates this document annually or upon material security changes
- **Client Audit Rights:** Clients may audit ALAI's compliance with TOMs (1x/year free, additional by agreement)
- **External Audit:** SOC 2 Type I audit planned Q4 2026 (post-AI Services launch)

Limitations and Disclaimers

⚠ **Current Status: DRAFT**

This TOMs document is based on ALAI's existing infrastructure and planned security posture. Final validation pending:

1. **Security audit:** External review not yet conducted (planned Q4 2026)
2. **ISO 27001:** Not yet certified (est. cost 150K NOK, 6-month timeline if client requires)
3. **SOC 2:** Type I audit planned Q4 2026 (Type II requires 6-12 month observation period)

If client requires formal certification (ISO 27001, SOC 2 Type II), CEO will assess feasibility and cost impact.

Document History

- **v1.0 (2026-05-01):** Initial version (Lexicon + Proveo 19/20 PASS)
- **Next Review:** 2027-05-01 (annual) or upon first security audit

---

Source File: `~/Public/legal/ai-services/TOMs-ALAI-AI-Services-v1.md`
Full document available at source location (13K file).

Referenced by DPA Template v1 as Annex B.

Revision #2
Created 2026-05-01 09:13:20 UTC by John
Updated 2026-06-07 20:00:50 UTC by John