DPA Template v1 (GDPR Article 28)

Data Processing Agreement (DPA)

Version: 1.0 | **Date:** 2026-05-01 | **Compliance:** GDPR Article 28, Norwegian Personal Data Act

---

Overview

This Data Processing Agreement (DPA) governs ALAI Holding AS' role as **Data Processor** when delivering AI services to clients who are **Data Controllers**.

GDPR Article 28(3) requires DPAs to specify 8 mandatory items. This template includes all 8.

When is a DPA Required?

Execute DPA if ALAI processes personal data on behalf of client:

- AI system processes customer names, emails, or IDs
- AI training uses client employee data
- System logs contain IP addresses or user activity
- Client explicitly requests GDPR compliance documentation

Skip DPA if:

- Pure technical audit (code review, architecture assessment) with no personal data access
- AI model training on fully anonymized datasets
- Consulting engagement with no data processing

GDPR Article 28(3) Mandatory Items

#	Requirement	Template Section	Proveo Status
1	Subject matter	2.1 (AI services)	✓ PASS
2	Duration	2.2 (duration of main agreement)	✓ PASS
3	Nature & purpose	2.3 (data types listed)	✓ PASS
4	Type of personal data	2.3 (identification, business, technical, AI training)	✓ PASS
5	Categories of data subjects	2.4 (customers, employees, end-users)	✓ PASS
6	Obligations of controller	Section dedicated to controller rights	✓ PASS
7	Authorization of sub-processors	3.4 (table + 30-day notice clause)	✓ PASS
8	Processor obligations	Section 3 (comprehensive)	✓ PASS

Sub-Processors

ALAI uses the following approved sub-processors:

Vendor	Service	Location	Safeguards
Anthropic PBC	AI model API (Claude)	USA (AWS us-east-1)	SOC 2 Type II, GDPR DPA, **Standard Contractual Clauses (SCCs)**
Microsoft Azure	Cloud infrastructure, hosting	EU West / Norway East	ISO 27001, SOC 2, GDPR compliant, Microsoft DPA
Cloudflare Inc.	CDN, DDoS protection, DNS	Global (EU data residency)	ISO 27001, SOC 2 Type II, GDPR DPA
Brevo	Transactional email	EU (Frankfurt)	GDPR compliant, ISO 27001

⚠ **NOTE:** Actual SCC documents from Anthropic are PENDING (see `dpa-vendor-log.md`). CEO must collect these before executing DPA with clients.

30-day notice rule: ALAI will notify clients 30 days before adding/changing sub-processors. Clients may object within this period.

Key Timelines

Event	Deadline	Notes
Breach notification	24 hours	ALAI notifies client of personal data breach within 24h of discovery
Data deletion/return	30 days	Upon contract termination, ALAI deletes or returns all personal data within 30 days
Audit response	14 days	ALAI responds to client audit questions within 14 days
Sub-processor change notice	30 days	Clients receive 30-day advance notice before sub-processor changes

Technical and Organizational Measures (TOMs)

The DPA references **Annex B: TOMs** which documents ALAI's security measures:

- **Encryption:** TLS 1.3 (transit), AES-256 (rest)
- **Access control:** MFA for all production access
- **Logging:** All personal data access logged
- **Backups:** Daily backups, 24h recovery time
- **Training:** Annual GDPR training for staff
- **Penetration testing:** Annual external security testing

Full TOMs document: TOMs ALAI AI Services v1

Audit Rights

Clients have the right to audit ALAI's compliance with this DPA:

- **Frequency:** Once per year without cost to client
- **Additional audits:** By agreement, with reasonable cost coverage
- **Access:** Client or designated representative may access ALAI premises and systems
- **Response time:** ALAI responds to audit questions within 14 days

Cross-Border Data Transfers

Non-EEA transfers: Anthropic (USA) processes data outside EEA. This requires **Standard Contractual Clauses (SCCs)** per GDPR Chapter V.

Status: DPA template references SCCs (section 5.1). CEO must obtain actual SCC documents from Anthropic before executing client DPAs.

Action Required: See `dpa-vendor-log.md` for draft vendor email. CEO must send and track responses.

Proveo Legal Review Status

Proveo review (2026-05-01): **19/20 PASS**

Critical Item	Status
GDPR Art.28 mandatory items (all 8 present)	✓ PASS
Sub-processor list complete	✓ PASS
24h breach notification + 30d deletion realistic	✓ PASS
Audit rights defined	✓ PASS
SCCs for non-EEA referenced	✓ PASS (reference) | ⚠ Documents pending
TOMs Annex B referenced	✓ PASS

Known Gap: SnowIT relationship undocumented. If SnowIT processes client data, SnowIT must be added to sub-processor list. Separate workstream required.

Usage Workflow

1. **CEO confirms engagement involves personal data processing**
2. **CEO fills template variables:** Client name/org.nr, data types (section 2.3), data subject categories (section 2.4)
3. **Attach TOMs as Annex B**
4. **Upload DPA + TOMs to Documenso** (two-document bundle)
5. **Client review:** May request security changes (e.g., ISO 27001 certification, on-premise deployment)
6. **CEO escalates material changes to Lexicon**
7. **Both parties sign via Documenso**
8. **Archive signed DPA + TOMs to Paperless-ngx** with tags: `legal-contract`, `dpa`, `gdpr`, `ai-services`

Full Template

Source File: `~/Public/legal/ai-services/DPA-template-v1.md`

Full bilingual template available at source location (23K file). Contact CEO for access or see client onboarding workflow.

For client onboarding process, see Client Onboarding Checklist.

Revision #2
Created 2026-05-01 09:12:00 UTC by John
Updated 2026-06-07 20:00:49 UTC by John