Legal Templates v1

Contract templates for AI Services client engagements. All templates bilingual (NO/EN). Norwegian text legally binding.

- Mutual NDA Template v1
- Retainer Contract Template v1
- DPA Template v1 (GDPR Article 28)
- TOMs ALAI AI Services v1
- Client Onboarding Checklist
- Documenso Upload Guide

Mutual NDA Template v1

GJENSIDIG TAUSHETSERKLÆRING / MUTUAL NON-DISCLOSURE AGREEMENT

Versjon / Version: 1.0
Dato / Date: 2026-05-01
Jurisdiksjon / Jurisdiction: Norge / Norway

NO: GJENSIDIG TAUSHETSERKLÆRING

1. Parter / Parties

Part 1:

- Navn: ALAI Holding AS
- Org.nr: 933 534 262
- Adresse: Tømmerrenna 1B, 2050 Jessheim, Norge
- Kontaktperson: Alem Akšamija
- E-post: alem@alai.no

Part 2:

- Navn: [PART_2_NAME]
- Org.nr: [PART_2_ORG_NUMBER]
- Adresse: [PART_2_ADDRESS]
- Kontaktperson: [PART_2_CONTACT_PERSON]
- E-post: [PART_2_EMAIL]

2. Formål

Partene ønsker å utveksle fortrolig informasjon i forbindelse med:

[BESKRIVELSE AV FORMÅL — f.eks. «vurdering av AI-tjenester, gjennomgang av kildekode, diskusjon av AI-agentløsninger, eller annet samarbeid»]

3. Definisjon av fortrolig informasjon

Fortrolig informasjon omfatter, men er ikke begrenset til:

- **Kildekode, algoritmer, og teknisk dokumentasjon** — inkludert AI-agentarkitektur, treningsdata, modellkonfigurasjon, og systemdesign
- **Forretningsinformasjon** — prising, kundelister, forretningsmuligheter, strategiske planer, finansielle data
- **AI-agentutdata** — generert innhold, analyseresultater, anbefalinger produsert av AI-systemer under evaluering eller utvikling
- **Tekniske spesifikasjoner** — API-dokumentasjon, integrasjonsplaner, infrastrukturkonfigurasjon
- **Immaterielle rettigheter** — oppfinnelser, patenter, varemerker, designmønstre
- **Annen informasjon** merket som «Fortrolig», «Confidential», eller som partene med rimelighet burde forstå er konfidensiell

Unntak:
Informasjon er IKKE fortrolig dersom den:

1. Er offentlig tilgjengelig på tidspunktet for utlevering, eller blir det senere uten at mottakende part har brutt denne avtalen
2. Var i mottakende parts besittelse før utlevering (dokumentert bevis)
3. Mottas fra en tredjepart uten bruddsforpliktelse
4. Er utviklet uavhengig av mottakende part uten bruk av fortrolig informasjon (dokumentert bevis)
5. Må utleveres etter lov eller rettskjennelse (med varsel til utleverende part)

4. Forpliktelser

Hver part forplikter seg til å:

1. **Beskytte fortrolig informasjon** med samme grad av forsiktighet som for egen fortrolig informasjon, minimum rimelig forsvarlig standard
2. **Kun bruke informasjonen** til formålet beskrevet i punkt 2
3. **Begrense tilgang** til ansatte, konsulenter, og underleverandører som har reelt behov (need-to-know) og som er bundet av tilsvarende taushetserklæring

4. **Ikke kopiere eller reprodusere** informasjonen uten skriftlig samtykke fra utleverende part, bortsett fra kopier nødvendig for formålet
5. **Returnere eller slette** all fortrolig informasjon ved avtaleforholdets opphør, eller på forespørsel fra utleverende part

5. Ingen lisens eller eierskap

Denne avtalen gir IKKE:

- Lisens til immaterielle rettigheter
- Eierskap til fortrolig informasjon
- Rett til å bruke informasjonen utover formålet i punkt 2

All fortrolig informasjon forblir utleverende parts eiendom.

6. Varighet

Taushetsplikten gjelder fra signeringsdato og i **2 (to) år** etter siste utlevering av fortrolig informasjon.

Forpliktelsene i punkt 4.5 (retur/sletting) trer i kraft ved avtalens opphør eller på forespørsel.

7. Brudd og erstatning

Ved brudd kan utleverende part:

1. Kreve umiddelbar stans (midlertidig forføyning)
2. Kreve erstatning for direkte tap
3. Kreve tilbakelevering av all fortrolig informasjon

Mottakende part er ansvarlig for brudd begått av egne ansatte, konsulenter, og underleverandører.

8. Lovvalg og verneting

Denne avtalen er underlagt **norsk rett**.

Tvister skal løses ved **Oslo tingrett** som eksklusivt verneting.

9. Diverse

9.1 Endringer
Endringer krever skriftlig tillegg signert av begge parter.

9.2 Oppdeling
Dersom en bestemmelse er ugyldig, forblir resten av avtalen i kraft.

9.3 Hele avtalen
Denne avtalen utgjør hele avtalen om taushetsplikt mellom partene og erstatter alle tidligere avtaler.

EN: MUTUAL NON-DISCLOSURE AGREEMENT

NOTE: The Norwegian text above is the legally binding version. This English translation is provided for reference only.

1. Parties

Party 1:

- Name: ALAI Holding AS
- Org.No: 933 534 262
- Address: Tømmerrenna 1B, 2050 Jessheim, Norway
- Contact Person: Alem Akšamija
- Email: alem@alai.no

Party 2:

- Name: [PART_2_NAME]
- Org.No: [PART_2_ORG_NUMBER]
- Address: [PART_2_ADDRESS]
- Contact Person: [PART_2_CONTACT_PERSON]
- Email: [PART_2_EMAIL]

2. Purpose

The parties wish to exchange confidential information in connection with:

[DESCRIPTION OF PURPOSE]

3. Definition of Confidential Information

Confidential Information includes, but is not limited to:

- **Source code, algorithms, and technical documentation** — including AI agent architecture, training data, model configuration, and system design
- **Business information** — pricing, customer lists, business opportunities, strategic plans, financial data
- **AI agent outputs** — generated content, analysis results, recommendations produced by AI systems under evaluation or development
- **Technical specifications** — API documentation, integration plans, infrastructure configuration
- **Intellectual property** — inventions, patents, trademarks, design patterns
- **Other information** marked as "Confidential" or that the parties should reasonably understand to be confidential

Exceptions:
Information is NOT confidential if:

1. It is publicly available at the time of disclosure, or becomes so later without breach of this agreement by the receiving party
2. It was in the receiving party's possession before disclosure (documented evidence)
3. It is received from a third party without breach obligation
4. It is independently developed by the receiving party without use of confidential information (documented evidence)
5. It must be disclosed by law or court order (with notice to the disclosing party)

See Norwegian version for complete terms. For signing workflow, upload to Documenso per Upload Guide.

Source File: ~/Public/legal/ai-services/MUTUAL-NDA-template-v1.md
Proveo Review: 19/20 PASS (2026-05-01)
ALAI Org.Nr: 933 534 262

Retainer Contract Template v1

AI Services Retainer Agreement

Version: 1.0 | **Date:** 2026-05-01 | **Jurisdiction:** Norway

---

Overview

This retainer agreement establishes the commercial framework for ongoing AI services delivery to clients. The agreement includes:

- **Monthly retainer model** (40-80K NOK per approved AI Services pricing)
- **3-month binding period** with 30-day termination notice thereafter
- **IP assignment trigger**: Transfer upon invoice payment (protects ALAI from non-payment)
- **Liability cap**: Sum of payments received in last 6 months
- **Governing law**: Norwegian law, Oslo District Court venue

Key Commercial Terms

Term	Value	Notes
Monthly retainer	[BELØP] NOK eks. mva.	Template variable — fill per engagement
Hourly overage rate	[TIMEPRIS] NOK eks. mva.	For hours exceeding retainer allocation
Payment terms	Net 14 days	Standard ALAI terms
Unused hours rollover	90 days	Then expire
Binding period	3 months minimum	Then monthly termination with 30d notice
Breach termination	14 days cure period	Immediate termination if not remedied

Template Structure

The full template is bilingual (Norwegian/English), with **Norwegian text legally binding**. English translation is for reference only.

Norwegian Sections (Legally Binding)

1. **Parter** — ALAI Holding AS (933 534 262) + Client details
2. **Formål og omfang** — AI services scope: audit, development, architecture, integration, training
3. **Retainer-modell** — Monthly fee, included hours, rollover rules, overage billing
4. **Betalingsvilkår** — Invoicing cycle, payment deadline, late interest
5. **Immaterielle rettigheter** — IP transfer to client upon payment; ALAI retains platform/tools
6. **Konfidensialitet** — References NDA (prerequisite) and DPA (if personal data processing)
7. **Ansvar** — Liability cap (6-month payments), no indirect loss liability
8. **Garantier** — Professional standards, no known vulnerabilities, 30-day complaint period
9. **Varighet** — 3-month binding + monthly thereafter, 30-day notice
10. **Force majeure** — Standard clause
11. **Lovvalg** — Norwegian law, Oslo tingrett venue

Annexes

- **Annex A:** Statement of Work (SoW) — per engagement, defines deliverables/milestones
- **Annex B:** Mutual NDA (see NDA Template)
- **Annex C:** Data Processing Agreement (see DPA Template)

Proveo Legal Review Status

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

Item	Status
Liability cap (NOK-denominated, 6-month payment sum)	✓ PASS
IP assignment trigger = on payment (not on signing)	✓ PASS
30-day notice + 3-month binding period	✓ PASS
Governing law (Norwegian) + Oslo tingrett venue	✓ PASS
Pricing alignment with AI Services tiers (40-80K)	✓ PASS
Bilingual consistency (NO/EN)	✓ PASS

Usage Workflow

1. **CEO fills template variables:** [BELØP], [TIMEPRIS], [ANTALL] hours, client name/org.nr/address
2. **CEO drafts first SoW (Annex A):** Specific deliverables, timeline, acceptance criteria
3. **Upload to Documenso:** Per Upload Guide
4. **Client negotiation:** If terms change, CEO escalates material legal changes to Lexicon for review
5. **Both parties sign via Documenso**
6. **Archive signed PDF to Paperless-ngx** with tags: `legal-contract`, `retainer`, `ai-services`, `[CLIENT_NAME]`
7. **Record in archive-first-ledger.jsonl** per ZAKON ARCHIVE FIRST

Full Template

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

Full bilingual template available at source location (15K file). Contact CEO for access or see client onboarding workflow.

For client onboarding process, see Client Onboarding Checklist.

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.

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.

Client Onboarding Checklist

AI Services Client Onboarding Checklist

Version: 1.0 | **Date:** 2026-05-01 | **Owner:** CEO + John + Lexicon

---

Overview

This checklist covers the complete client onboarding journey from initial contact through first invoice and project kickoff.

Total Estimated Duration: 7-14 business days (contract-to-kickoff) | 2-6 weeks (contract-to-first-delivery)

Phase 1: Pre-Contract Documentation

Step 1.1: Mutual NDA Execution

Owner: CEO | **Duration:** 1-3 days

1. CEO fills NDA template with client details
2. Upload to Documenso (sign.basicconsulting.no)
3. Both parties sign
4. Archive signed PDF to Paperless-ngx with tags: `legal-contract`, `nda`, `ai-services`, `[CLIENT_NAME]`
5. Record in `~/system/state/archive-first-ledger.jsonl`

✓ **Done when:** Signed NDA archived + ledger entry created

Step 1.2: Retainer Agreement + SoW Negotiation

Owner: CEO (commercial), Lexicon (legal if amended) | **Duration:** 3-5 days

1. CEO defines:
   - Monthly retainer: [BELØP] NOK (range 40-80K per approved pricing)
   - Hourly overage rate: [TIMEPRIS] NOK
   - Included hours per month: [TIMER]
   - First Statement of Work (SoW): Deliverables, milestones, timeline
2. CEO fills Retainer template
3. CEO drafts first SoW (Appendix A)
4. Upload to Documenso → client reviews
5. If client requests material legal changes → Lexicon reviews
6. Both parties sign
7. Archive signed Retainer + SoW to Paperless-ngx with tags: `legal-contract`, `retainer`, `ai-services`

✓ **Done when:** Signed Retainer + SoW archived, pricing confirmed, 3-month binding period start date recorded

---

Phase 2: Data Protection Compliance

Step 2.1: DPA Execution (if processing personal data)

Owner: CEO (execution), Lexicon (GDPR review) | **Duration:** 2-5 days

Decision Point: Does engagement involve processing personal data?

- **YES** → Execute DPA (required by GDPR Article 28)
- **NO** → Skip to Phase 3

Actions (if DPA required):

1. CEO confirms data types with client (identification, business, technical logs, AI training data)
2. CEO fills DPA template:
   - Section 2.3: Data types
   - Section 2.4: Data subject categories
3. Attach TOMs as Annex B
4. Upload DPA + TOMs to Documenso (two-document bundle)
5. Client reviews → may request security changes (ISO 27001, on-premise deployment)
6. CEO escalates material changes to Lexicon

7. Both parties sign
8. Archive signed DPA + TOMs to Paperless-ngx with tags: `legal-contract`, `dpa`, `gdpr`, `ai-services`

✓ **Done when:** Signed DPA archived with TOMs annex, sub-processor disclosure delivered

Blocking Issues:

- Client requires ISO 27001 → CEO decision (cost ~150K NOK, 6-month timeline)
- Client prohibits non-EEA sub-processors → CEO assesses if Anthropic can be replaced with EU-hosted LLM
- Healthcare/finance client → Escalate to Lexicon (HIPAA, PCI-DSS compliance)

Phase 3: Financial Setup

Step 3.1: First Invoice Issuance

Owner: CEO | **Duration:** 1 day

1. CEO creates client in Fiken (fiken.no):
   - Client name, org.nr, billing address, email
   - Payment terms: Net 14 days (standard ALAI)
   - Monthly recurring invoice flag
2. CEO issues Invoice #1:
   - Line item: "AI Services Retainer — [MONTH] [YEAR]"
   - Amount: [BELØP] NOK eks. mva.
   - Due date: 14 days from invoice date
3. Invoice auto-sent via Fiken to client email
4. CEO confirms client received invoice

✓ **Done when:** Invoice sent, client acknowledges receipt

Step 3.2: Payment Confirmation

Owner: CEO | **Duration:** 0-14 days

1. CEO monitors Fiken for incoming payment
2. Once payment received:
   - Confirm amount matches invoice
   - Confirm payment reference includes invoice number
3. If payment overdue (14+ days) → CEO sends reminder
4. If 30+ days overdue → CEO pauses work per Retainer clause (IP transfer = on payment)

✓ **Done when:** First retainer payment received + recorded in Fiken

---

Phase 4: Project Kickoff

Step 4.1: Technical Onboarding Call

Owner: CEO (kickoff), John (orchestration), Specialist Agents (delivery) | **Duration:** 1-2 hours

1. CEO schedules kickoff call with:
   - Client PM/Tech Lead
   - ALAI: CEO + John (if technical deep-dive)
2. **Agenda:**
   - Review signed SoW deliverables and timeline
   - Confirm data access requirements (API keys, database credentials, codebase access)
   - Establish communication channels (Slack, email, video calls)
   - Agree on meeting cadence (weekly status, bi-weekly demo)
   - Set first milestone delivery date
3. CEO documents meeting notes → share with client
4. John creates Mission Control tasks for first SoW deliverables:
   - Task owner: Specialist agent (Codecraft, Vizu, Architect)
   - Priority: H (client deliverable)
   - Deadline: Per SoW milestone

✓ **Done when:** Kickoff call completed, client access received, MC tasks created, first milestone scheduled

Step 4.2: First Deliverable Milestone

Owner: Specialist Agents (execution), Proveo (validation), CEO (client acceptance) | **Duration:** Per SoW (typically 1-4 weeks)

1. Specialist agents execute first SoW deliverable
2. Proveo validates per acceptance criteria in SoW
3. John marks MC task as ready_for_review
4. CEO reviews internally
5. CEO submits deliverable to client
6. Client reviews and provides feedback
7. If revisions needed → agents execute, Proveo re-validates, CEO re-submits
8. Client formally accepts deliverable
9. CEO archives deliverable to Paperless-ngx with tags: `client-deliverable`, `ai-services`, `[CLIENT_NAME]`

✓ **Done when:** Client accepts deliverable, deliverable archived, next milestone scheduled

---

Phase 5: Ongoing Engagement

Monthly Retainer Rhythm

Monthly Cycle:

1. **Day 1:** CEO issues retainer invoice for current month via Fiken
2. **Day 14:** Payment due
3. **Week 1-4:** Agents execute SoW tasks within retainer hours
4. **End of month:** CEO reviews time tracking:
   - Hours < retainer allocation → carry-forward or lose (per Retainer clause 3.3)
   - Hours > retainer allocation → invoice overage at [TIMEPRIS] NOK/hour
5. **Monthly status report:** CEO sends client:
   - Hours used vs. allocated
   - Deliverables completed
   - Next month's planned work

Contract Renewal or Termination

At 3-Month Binding Period End:

- CEO checks client satisfaction
- If renewing → Continue monthly retainer (auto-renews unless 30-day notice)
- If terminating → CEO sends 30-day written notice per Retainer clause 6.2

Upon termination:

1. Complete all in-flight SoW tasks
2. Execute DPA data deletion/return (30-day deadline per DPA section 3.7)
3. Final invoice for any unpaid overages
4. Archive all signed contracts and deliverables per ZAKON ARCHIVE FIRST

Timeline Summary

Phase	Step	Duration	Owner
Pre-Contract	NDA signing	1-3 days	CEO

Phase	Step	Duration	Owner
Pre-Contract	Retainer + SoW negotiation	3-5 days	CEO
Data Protection	DPA execution	2-5 days	CEO + Lexicon
Financial	First invoice issuance	1 day	CEO
Financial	Payment confirmation	0-14 days	CEO
Kickoff	Technical onboarding	1-2 hours	CEO + John
Kickoff	First deliverable	1-4 weeks	Agents + Proveo
TOTAL	**Contract-to-kickoff**	**7-14 days**	—
TOTAL	**Contract-to-first-delivery**	**2-6 weeks**	—

Decision Trees

Does this engagement require a DPA?

YES if:

- 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

NO if:

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

What if client requests custom contract terms?

1. **Minor changes** (formatting, address corrections) → CEO approves directly
2. **Commercial changes** (pricing, payment terms) → CEO approves if within standard bounds
3. **Legal changes** (liability cap removal, IP assignment reversal) → CEO escalates to Lexicon
4. **Security changes** (ISO 27001, on-premise) → CEO escalates to John for technical impact analysis

Timeline Impact:

- Minor: +0 days
- Commercial: +1-2 days
- Legal: +3-5 days (Lexicon review)
- Security: +1-2 weeks (technical assessment)

Tools and References

Required Systems

- **Documenso:** sign.basicconsulting.no (contract signing)
- **Paperless-ngx:** archive.alai.no (archiving per ZAKON ARCHIVE FIRST)
- **Fiken:** fiken.no (invoicing and payment tracking)
- **Mission Control:** `node ~/system/tools/mc.js` (task tracking)
- **Bitwarden:** Client credential storage (if access keys provided)

Document Templates

- Mutual NDA Template v1
- Retainer Contract Template v1
- DPA Template v1
- TOMs ALAI AI Services v1

Legal Review

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

Known gap: SnowIT relationship undocumented (separate workstream — does not block client onboarding)

Open Questions for CEO

1. Should we engage a Norwegian law firm for final template review before first client use? (Est. cost: 10-15K NOK, timeline: 1-2 weeks)
2. Do we have professional indemnity insurance covering AI services?
3. If SnowIT developers access client data, should SnowIT be added to DPA sub-processor list?

4. If a client requires ISO 27001 certification, what is the go/no-go decision point? (Cost: ~150K NOK, timeline: 6 months)

Document Owner: Skillforge
Last Updated: 2026-05-01
Review Cycle: Quarterly (or upon first client feedback)

Documenso Upload Guide

Documenso Template Upload Guide

Purpose: Manual upload instructions for ALAI AI Services legal templates to Documenso (sign.basicconsulting.no).

Date: 2026-05-01 | **Prepared by:** Lexicon

Templates to Upload

The following three templates must be uploaded as **DRAFT templates** ready for client signing:

1. **Mutual NDA** (Gjensidig Taushetserklæring)
2. **Retainer Contract** (Ramme-avtale)
3. **Data Processing Agreement (DPA)**

Pre-Upload Preparation

Step 1: Convert Markdown to PDF

Use Pandoc or LibreOffice to convert `.md` files to `.pdf`:

```
# Using Pandoc (if installed)
pandoc ~/Public/legal/ai-services/MUTUAL-NDA-template-v1.md \
  -o ~/Public/legal/ai-services/MUTUAL-NDA-template-v1.pdf \
  --pdf-engine=xelatex \
  -V geometry:margin=2.5cm \
  -V fontsize=11pt

pandoc ~/Public/legal/ai-services/RETAINER-CONTRACT-template-v1.md \
```

```
  -o ~/Public/legal/ai-services/RETAINER-CONTRACT-template-v1.pdf \
  --pdf-engine=xelatex \
  -V geometry:margin=2.5cm \
  -V fontsize=11pt

pandoc ~/Public/legal/ai-services/DPA-template-v1.md \
  -o ~/Public/legal/ai-services/DPA-template-v1.pdf \
  --pdf-engine=xelatex \
  -V geometry:margin=2.5cm \
  -V fontsize=11pt
```

Alternative: Open `.md` files in text editor, copy content to Google Docs or LibreOffice, export as PDF.

Documenso Upload Workflow

Step 2: Log in to Documenso

1. Navigate to: **https://sign.basicconsulting.no**
2. Log in with ALAI admin credentials (use Bitwarden: `bw get item "Documenso - sign.basicconsulting.no"`)

Step 3: Create Template (for each document)

For MUTUAL-NDA-template-v1.pdf:

1. Click **"Templates"** in left sidebar
2. Click **"Create Template"**
3. **Upload PDF:** Select `MUTUAL-NDA-template-v1.pdf`
4. **Template Name:** `AI Services - Mutual NDA (NO/EN)`
5. **Add Signature Fields:**
   - **Signer 1 (ALAI Holding AS):**
     - Signature field at "For ALAI Holding AS" signature line
     - Name field at "Navn / Name" line
     - Date field at "Dato / Date" line
   - **Signer 2 (Client):**
     - Signature field at "For [PART_2_NAME]" signature line
     - Name field at "Navn / Name" line
     - Date field at "Dato / Date" line
6. **Add Text Fields for Variables:**

- `[PART_2_NAME]` — Text field at top (Part 2 section)
- `[PART_2_ORG_NUMBER]` — Text field
- `[PART_2_ADDRESS]` — Text field
- `[PART_2_CONTACT_PERSON]` — Text field
- `[PART_2_EMAIL]` — Email field
- `[BESKRIVELSE AV FORMÅL]` — Large text area (NO version, section 2)
- `[DESCRIPTION OF PURPOSE]` — Large text area (EN version, section 2)

7. **Save as Draft Template**
8. **Test:** Create a test submission to verify all fields populate correctly

Repeat for RETAINER-CONTRACT-template-v1.pdf:

- Template Name: `AI Services - Retainer Contract (NO/EN)`
- Variables: `[KUNDE_NAVN]`, `[KUNDE_ORG_NUMMER]`, `[KUNDE_ADRESSE]`, `[KUNDE_KONTAKTPERSON]`, `[KUNDE_EPOST]`, `[BELØP]`, `[ANTALL]`, `[TIMEPRIS]`
- Signature fields: ALAI + Client

Repeat for DPA-template-v1.pdf:

- Template Name: `AI Services - Data Processing Agreement (DPA)`
- Variables: `[KUNDE_NAVN]`, `[KUNDE_ORG_NUMMER]`, etc., `[DATO]`
- Signature fields: Data Controller (Client) + Data Processor (ALAI)

Step 4: Archive Templates

After templates are created in Documenso:

1. **Export templates as PDFs** from Documenso (if possible)
2. **Upload to archive.alai.no** (Paperless-ngx):
   - Tag: `legal-template`, `ai-services`, `documenso`
   - Correspondent: `ALAI Holding AS`
   - Document type: `Contract Template`
3. **Update ledger:** Append to `~/system/state/archive-first-ledger.jsonl`

Step 5: Test Workflow

1. Create a **test submission** with dummy client data:
   - Test Client Name: "Test AS"
   - Test Email: post@alai.no (CEO mailbox)
2. Send signature request
3. Verify:

- Email branding is correct
- All fields populate
- Signature flow works
- Signed PDF is retrievable

4. **Delete test submission** after verification

Alternative: API Upload (Future Enhancement)

Current blocker: Documenso API authentication not yet tested in CLI context.

Future workflow (when API ready):

```
# Get Documenso API key from Bitwarden
DOCUMENSO_API_KEY=$(bw get password "Documenso API Key")

# Upload template via API (endpoint TBD — check Documenso docs)
curl -X POST https://sign.basicconsulting.no/api/v1/templates \
  -H "Authorization: Bearer $DOCUMENSO_API_KEY" \
  -F "file=@~/Public/legal/ai-services/MUTUAL-NDA-template-v1.pdf" \
  -F "name=AI Services - Mutual NDA"
```

Task for future: Create `~/system/tools/documenso-template-upload.js` to automate this.

Notes

Bismillah and ALAI branding:
Ensure PDF templates include:

- ALAI logo in header (if Documenso supports custom branding)
- Bismillah invocation at top of first page (already in Markdown source)

Signature notification:
Documenso webhook at `https://api.basicconsulting.no/webhooks/documenso` will trigger on `DOCUMENT_COMPLETED` event. Webhook will:

- Post to Slack #exec
- Comment on MC task (if `#XXXX` in document title)

- Emit event to event-bus

Future automation:
Once signed, document should be auto-uploaded to archive.alai.no (see SENTINEL v3 audit Wire 2+3). Current state: manual upload required.

Full Source File: `~/Public/legal/ai-services/documenso-upload-guide.md`