Legal & Marketing Constraints When Outsourcing Security

Legal & Marketing Constraints When Outsourcing Security

⚠ **DISCLAIMER:** This is general industry knowledge. For authoritative legal advice, consult Norwegian advokat (Wiersholm/BAHR/Schjødt security practice) before signing any MSA or sub-contract.

Legal Requirements (White-label Model)

1. Master Services Agreement (MSA) with Partner

Back-to-back clauses — every obligation ALAI accepts from client must flow through to partner.

2. Sub-Processor DPA (GDPR Art.28)

Partner processes client personal data → must sign Sub-Processor Data Processing Agreement under GDPR Article 28.

3. NDA Chain

Partner must sign client-equivalent NDA. If client requires special classification (e.g., NSM Fortrolig), partner must hold equivalent clearance.

4. Right-to-Audit Clause

ALAI must have contractual right to audit partner's security practices. If partner refuses this clause → RED FLAG.

5. Cyber Liability Insurance Back-to-Back

Partner must carry cyber liability insurance coverage equivalent to ALAI's policy (minimum 5-10M NOK). ALAI must verify partner's insurance certificate annually.

6. IP Clause

- ALAI owns final report delivered to client
- Partner retains methodology and tooling IP

7. SLA Back-to-Back

If ALAI promises client "final report within 10 business days", partner must contractually promise ALAI "draft report within 7 business days".

8. Partner-Cert Legitimacy Clause

Partner guarantees active CREST/NSM/PCI certification during engagement period. If certification lapses, ALAI has termination right.

Norwegian Employment Law Constraint

Arbeidsmiljøloven §14-12 / §14-13 ("Innleie")

If partner sends individual testers to work under ALAI's direction (vs. partner delivering service as independent firm), Norwegian law may classify this as employment leasing.

Mitigation: Structure contract as firm-to-firm B2B service delivery. Partner retains operational control over testers. ALAI engages partner for deliverable (pen-test report), NOT for staff augmentation.

Marketing Do's and Don'ts

? Permitted Claims

- "Delivered in partnership with [X]"
- "Powered by [X]"
- "ALAI coordinates security testing through certified partners"

? Prohibited Claims

- "ALAI is CREST-certified" (false — partner is, ALAI is not)
- "ALAI is NSM Sikkerhetsgodkjent" (false — unless ALAI itself holds clearance)
- "ALAI performs pen-tests" (technically partner performs, ALAI coordinates)

?? Special Constraints for Specific Certifications

NSM Sikkerhetsgodkjent Work (Classified)

Only certified firms can deliver classified security work. ALAI CANNOT promise this unless ALAI itself obtains NSM clearance (12-24 month process).

PCI ASV Scan

Payment Card Industry Approved Scanning Vendor (ASV) reports must be signed directly by ASV firm. ALAI cannot white-label PCI ASV scans — client must contract ASV directly (or ALAI refers under Model 1).

What You CANNOT Promise to Client

- NSM Sikkerhetsgodkjent delivery (unless ALAI holds clearance)
- PCI ASV scan under ALAI name (ASV firm must sign report)
- Specific tester by name (partner retains operational control)

Related: Outsource Models, Practical First Steps

Source: MC #10446, CEO email 2026-05-01 (Message-ID 4929b145)

Revision #3
Created 2026-05-01 19:14:04 UTC by John
Updated 2026-06-07 20:00:55 UTC by John