Compliance Overview

> Last Verified: 2026-02-17 | Owner: John

Drop — Compliance Overview

Regulatory Framework

PSD2 Compliance

- **AISP (Account Information Service Provider)** — Read bank account balances via Open Banking
- **PISP (Payment Initiation Service Provider)** — Initiate payments from user's bank account
- **No e-money licence required** — Pass-through model avoids holding funds

AML/KYC Requirements

- **BankID verification** — Mandatory before any transaction (satisfies Strong Customer Authentication)
- **Transaction monitoring** — screening.ts service for suspicious activity
- **STR reporting** — str.ts service for Suspicious Transaction Reports
- **7-year retention** — data-retention.ts service for compliance

GDPR Compliance

- **Data minimization** — Only collect necessary data
- **User rights** — Rectification, restriction, objection, erasure APIs implemented
- **Consent management** — BankID consent for Open Banking access
- **Data retention** — Automatic deletion after retention period
- **Privacy page** — /personvern page with full transparency

Incident Response

Beredskapsplan (Contingency Plan)

Location: `/Users/makinja/ALAI/products/Drop/legal/beredskapsplan.md`

Key Elements:

1. **Incident classification** — P1 (critical) to P4 (minor)
2. **Response team** — Roles and responsibilities
3. **Communication protocol** — Internal and external notifications
4. **Recovery procedures** — System restoration steps
5. **Post-incident review** — Root cause analysis, lessons learned

Hendelseshaandtering (Event Handling)

Location: `/Users/makinja/ALAI/products/Drop/legal/hendelseshaandtering.md`

Covers:

- Security incidents (data breach, unauthorized access)
- Operational incidents (system outage, payment failures)
- Compliance incidents (regulatory violations)
- Escalation procedures
- Documentation requirements

Data Processing

Behandlingsprotokoll (Processing Protocol)

Location: `/Users/makinja/ALAI/products/Drop/legal/behandlingsprotokoll.md`

Defines:

- Data categories collected
- Processing purposes
- Legal basis (consent, contract, legal obligation)
- Data retention periods
- Security measures
- Third-party processors

Data Processing Agreements

Location: `/Users/makinja/ALAI/products/Drop/legal/`

Four DPA templates for different processor categories:

1. Banking partners (Wise, Swan)
2. Infrastructure providers (Vercel)
3. Analytics services
4. Support tools

Fees & Pricing

Gebyrskjema (Fee Schedule)

Location: `/Users/makinja/ALAI/products/Drop/legal/gebyrskjema.md`

Pricing:

- Remittance: 0.5% of transfer amount
- QR payments: 1% merchant fee, free for consumers
- Currency conversion: Mid-market rate + 0.3% markup
- Account linking: Free
- Failed payments: No charge

Rammeavtale (Framework Agreement)

Location: `/Users/makinja/ALAI/products/Drop/legal/rammeavtale.md`

Standard terms and conditions for Drop users.

Security Measures

Application Security

- **JWT RS256** — Asymmetric key authentication
- **httpOnly cookies** — XSS protection
- **CSP nonce** — Content Security Policy with nonces
- **Rate limiting** — API throttling
- **Input validation** — Parameterized SQL, schema validation

Infrastructure Security

- **CI/CD scanning** — Trivy vulnerability scanning
- **Secrets management** — Environment-based secret rotation
- **TLS everywhere** — HTTPS enforced
- **Database encryption** — At-rest encryption

Operational Security

- **Access control** — Role-based permissions
- **Audit logging** — All sensitive actions logged
- **Disaster recovery** — Backup and restore procedures (DR test plan)
- **Monitoring** — Real-time alerts for anomalies

Revision #3
Created 2026-02-17 22:16:14 UTC by John
Updated 2026-05-31 20:00:55 UTC by John