Compliance Gap Analysis

Drop Gap Analysis v2

Regulatory Compliance Gap Assessment

Date: 2026-02-12 **Prepared for:** ALAI Holding AS / Drop Payment App **Source code reviewed:** `/Users/makinja/ALAI/products/Drop/src/drop-app/src/` **Security rapport:** `/Users/makinja/ALAI/products/Drop/security/drop-security-rapport.md` **QA rapport:** `/Users/makinja/ALAI/products/Drop/project/docs/drop-qa-rapport.md`

> **NOTE (2026-03-03):** This analysis was performed on 2026-02-12. ADR-014 (2026-03-03) removed SQLite and replaced it with PostgreSQL 16 in all environments (AWS RDS, AES-256 at rest). All SQLite-specific gaps in this document (single-file DB, no HA, no backup, no retention policy tooling) are resolved by the PostgreSQL migration. Review and update this document against the current PostgreSQL 16 architecture.

Executive Summary

Drop is an MVP-stage Next.js payment app (remittance + QR payments) with SQLite backend. The codebase has solid fundamentals (parameterized SQL, JWT auth, atomic transactions) but has **zero regulatory compliance infrastructure**. Every regulatory area has critical gaps. The app cannot legally process a single real transaction in its current state.

Overall compliance readiness: 8/100

Area	Readiness	Critical Gaps
Licensing	0%	No license applied for, no agent arrangement

Area	Readiness	Critical Gaps
PSD2/SCA	10%	No BankID, no SCA, no Open Banking integration
AML/KYC	5%	Mock KYC only, no real identity verification, no transaction monitoring
GDPR	15%	Landing page has terms, but no DPIA, no processing register, limited privacy notice
ICT Security	25%	Basic security controls exist but no formal policies, no BCP, no pen tests
Governance	5%	No compliance officer, no internal control framework documented
Valutaregisteret	0%	No SSB registration, no reporting capability
Consumer Protection	10%	Basic terms exist but incomplete, no Finansklagenemnda membership

---

1. Licensing Gap Analysis

Current State

- No Finanstilsynet license applied for
- No agent arrangement with licensed institution
- App is running as a standalone MVP/demo

Gap Table

Requirement	Required State	Current State	Gap	Priority
Payment institution license	Valid license from Finanstilsynet	None	**FULL GAP**	CRITICAL
Client fund safeguarding	Segregated account or insurance	Not applicable (demo mode)	**FULL GAP**	CRITICAL
Initial capital	20,000-125,000 EUR depending on scope	Not secured	**FULL GAP**	CRITICAL
Business plan with projections	3-year financial plan	Exists as business case (`project/docs/zica-business-case-v2.md`)	PARTIAL -- needs licensing-format update	HIGH

Requirement	Required State	Current State	Gap	Priority
Agent arrangement (alternative)	Registered agent under licensed PSP	None	**FULL GAP**	CRITICAL

Recommendation

Fastest path to market: Establish agent arrangement with a licensed Norwegian payment institution while simultaneously preparing full license application. The agent model allows live transactions within 1-3 months; own license takes 6-12 months.

---

2. PSD2 / Betalingstjenesteloven Gap Analysis

Current State (from code review)

- **Auth:** `lib/auth.ts` -- JWT with HS256, cookie-based, 24h expiry
- **SCA:** None. Login is email + password only. No second factor.
- **BankID:** Not integrated. CLAUDE.md mentions it as a requirement but it is not implemented.
- **Open Banking:** Not integrated. Architecture doc mentions pass-through model but all balance/transaction data is local SQLite.
- **Fee disclosure:** Remittance shows fee (0.5%) and QR shows fee (1%) in API responses, but no pre-contractual disclosure framework.
- **Framework agreement:** Landing page has `vilkar.html` (terms) but not compliant with betalingstjenesteloven SS 3-1 format.

Gap Table

Requirement	Law Reference	Current State	Gap	Priority
Strong Customer Authentication	SS 4-28, 4-29	Email + password only (single factor)	**FULL GAP** -- No SCA	CRITICAL
BankID integration	SS 4-28 (Norwegian SCA)	Not implemented; mentioned in architecture doc	**FULL GAP**	CRITICAL
Dynamic linking (amount+payee to auth)	Del. Reg. Art. 5	Not implemented	**FULL GAP**	CRITICAL

Requirement	Law Reference	Current State	Gap	Priority
Open Banking AISP/PISP	SS 4-40 to 4-46	Not implemented; balance is local	**FULL GAP**	CRITICAL
Framework agreement	SS 3-1 to 3-8	Basic terms page exists (`vilkar.html`)	**PARTIAL** -- needs betalingstjenesteloven format	HIGH
Per-transaction receipt	SS 3-22 to 3-26	API returns transaction data; no formal receipt	**PARTIAL** -- needs formatting to comply	HIGH
Fee transparency pre-auth	SS 3-23	Fee shown in API response after submission	**GAP** -- fee must be shown BEFORE authorization	HIGH
Exchange rate disclosure	SS 3-24	Rate shown in API response; no reference rate markup	**PARTIAL** -- needs reference rate + markup	HIGH
Execution time disclosure	SS 4-15	Remittance returns `eta: "1-2 business days"` hardcoded	**PARTIAL** -- needs accurate per-corridor times	MEDIUM
Unauthorized transaction refund	SS 4-19 to 4-22	No refund mechanism exists	**FULL GAP**	HIGH
Session management / token revocation	Related to SCA	Sessions table exists but unused (`lib/db.ts:97-104`). Security report H1 confirms no revocation.	**FULL GAP**	HIGH

Technical Gaps in Code

File: `lib/auth.ts`

- Line 18-20: JWT_SECRET uses dev fallback in non-production. Production enforcement is correct.
- Line 48-54: Cookie settings are solid (httpOnly, secure, sameSite strict). Good foundation.
- **Missing:** No BankID callback handler, no OIDC/OAuth flow, no second factor.

File: `app/api/auth/register/route.ts`

- Line 20-29: Registration collects email, password, firstName, lastName, phone. No DOB field.
- Line 27: Password validation is length-only (>= 8 chars). No complexity requirements.
- **Missing:** Age verification (18+), BankID verification, Norwegian residency check.

File: `app/api/transactions/remittance/route.ts`

- Line 21: KYC check exists (`kyc_status !== "approved"` returns 403). Good gate, but KYC is fake.
- Line 60: Fee calculation (0.5%) is hardcoded. No disclosure step before authorization.
- **Missing:** Pre-authorization disclosure screen, SCA for transaction signing.

File: `app/api/transactions/qr-payment/route.ts`

- No KYC check (QA rapport H-11 confirms this). A user with pending KYC can make QR payments.
- **Missing:** KYC gate for QR payments, SCA for transaction signing.

---

3. AML / Hvitvaskingsloven Gap Analysis

Current State (from code review)

- **KYC:** `users.kyc_status` field exists (pending/approved/rejected) but verification is mocked.
- **Sumsub integration:** `lib/services/mock-sumsub.ts` -- fully mocked, no real API calls.
- **Transaction monitoring:** None. No rules, no alerts, no flagging.
- **STR filing:** No mechanism.
- **PEP/Sanctions screening:** None.
- **AML officer:** Not appointed.
- **Risk assessment:** Not conducted.

Gap Table

Requirement	Law Reference	Current State	Gap	Priority
AML risk assessment	SS 6, 7	Not conducted	**FULL GAP**	CRITICAL
AML policy & procedures	SS 8	Not created	**FULL GAP**	CRITICAL
AML compliance officer	SS 8(5)	Not appointed	**FULL GAP**	CRITICAL
Customer identity verification	SS 12	Mock only (`mock-sumsub.ts`); `kyc_status` field is manually set	**FULL GAP**	CRITICAL
BankID as identity verification	SS 12(3)	Not integrated	**FULL GAP**	CRITICAL

Requirement	Law Reference	Current State	Gap	Priority
Ongoing customer monitoring	SS 24	None	**FULL GAP**	CRITICAL
Transaction monitoring system	SS 24, 25	None -- no rules, no alerts	**FULL GAP**	CRITICAL
STR reporting to EFE	SS 26	No mechanism exists	**FULL GAP**	CRITICAL
PEP screening	SS 18	None	**FULL GAP**	CRITICAL
Sanctions screening	Sanctions regulations	None	**FULL GAP**	CRITICAL
Record keeping (5 years)	SS 30	SQLite local file, no retention policy	**PARTIAL** -- data stored but no policy	HIGH
Customer risk categorization	SS 12(4)	No risk model	**FULL GAP**	HIGH
Source of funds documentation	SS 17(2)	Not collected for any transaction	**FULL GAP**	HIGH
AML training	SS 36	No training program	**FULL GAP**	MEDIUM
Ongoing PEP/sanctions rescreening	SS 18(5), 24	None	**FULL GAP**	HIGH

Technical Gaps in Code

File: `lib/db.ts`

- Line 29: `kyc_status` field exists with proper enum. Good schema foundation.
- **Missing:** No `risk_level` column, no `pep_status`, no `sanctions_check_date`, no `kyc_verified_at`, no `kyc_method` (BankID vs document vs simplified).

File: `lib/services/mock-sumsub.ts`

- Entire file is a mock. Lines 204-224 show random 90% approval logic.
- Sumsub interface has proper checks modeled (documentAuthenticity, livenessCheck, facematch, sanctionsCheck, pepCheck) but all mocked.
- **Missing:** Real Sumsub API integration, BankID integration for Norwegian residents.

File: `app/api/transactions/remittance/route.ts`

- Line 21: KYC gate exists. Good.
- Line 40: Amount limits (100-50,000 NOK). Good.
- **Missing:** Transaction monitoring hooks, suspicious pattern detection, cumulative daily/monthly limit checks, corridor risk assessment.

Database schema missing tables:

- `aml_alerts` -- transaction monitoring alerts
- `str_reports` -- suspicious transaction report records
- `pep_screening_results` -- PEP check results per user
- `sanctions_screening_results` -- sanctions check results
- `customer_risk_profile` -- risk categorization per user
- `kyc_documents` -- verified identity documents
- `audit_log` -- comprehensive audit trail (also noted in security rapport L3)

---

4. GDPR / Personopplysningsloven Gap Analysis

Current State (from code review)

- Landing page has terms (`vilkar.html`) and presumably a privacy notice
- No DPIA conducted
- No Register of Processing Activities
- No data processing agreements with service providers
- No data subject rights procedures implemented
- No cookie consent mechanism
- No data retention schedule implemented

Gap Table

Requirement	GDPR Reference	Current State	Gap	Priority
DPIA	Art. 35	Not conducted	**FULL GAP**	CRITICAL
Privacy policy (nb)	Art. 13	Basic terms exist; unclear if full privacy notice	**PARTIAL**	CRITICAL
Register of processing activities	Art. 30	Not created	**FULL GAP**	HIGH
Lawful basis documentation	Art. 6	Not documented	**FULL GAP**	HIGH
Data processing agreements	Art. 28	None (no real processors yet, but mock services reference Swan, Stripe, Sumsub)	**FULL GAP** for production	HIGH

Requirement	GDPR Reference	Current State	Gap	Priority
SCCs for non-EEA transfers	Art. 46	Not prepared (remittance to RS, BA, TR, PK requires SCCs)	**FULL GAP**	HIGH
Transfer Impact Assessments	Schrems II	Not conducted	**FULL GAP**	HIGH
Data subject access procedure	Art. 15	No API endpoint or process for data access requests	**FULL GAP**	HIGH
Right to erasure procedure	Art. 17	No deletion capability (AML retention conflicts need mapping)	**FULL GAP**	HIGH
Data portability	Art. 20	No export mechanism	**FULL GAP**	MEDIUM
Cookie consent	Art. 6(1)(a), ePrivacy	No consent mechanism	**FULL GAP**	MEDIUM
Retention schedule	Art. 5(1)(e)	No schedule; data stored indefinitely	**FULL GAP**	MEDIUM
Data breach response plan	Art. 33-34	Not created	**FULL GAP**	HIGH
DPO appointment	Art. 37	Not appointed (may not be required for small PSP but recommended)	**GAP**	MEDIUM

Technical Gaps in Code

File: `lib/db.ts`

- All personal data stored in plaintext SQLite: name, email, phone, bank accounts, transaction history.
- Card data stored in plaintext (security rapport C1). PCI-DSS violation AND GDPR security adequacy issue.
- No encryption at rest.
- No field-level encryption for sensitive data.
- No `deleted_at` or soft-delete mechanism for data subject erasure.
- No data export endpoint.

File: `app/api/auth/register/route.ts`

- Collects personal data (email, name, phone) with no consent mechanism.
- No link to privacy policy during registration.

- No purpose disclosure.

Cross-border transfer data flow:

- Remittance sends data to recipients in RS, BA, TR, PK (non-EEA countries).
- No SCCs or TIAs prepared for these transfers.
- Recipient data (name, bank account) is processed for non-EEA delivery.

---

5. IKT-forskriften / DORA Gap Analysis

Current State (from security rapport and code review)

- JWT auth with proper cookie config (positive)
- Parameterized SQL throughout (positive)
- Security headers configured (CSP, X-Frame, X-Content-Type, Referrer-Policy, Permissions-Policy) (positive)
- Rate limiting exists but in-memory only (security rapport H2)
- No formal IT security policy document
- No BCP/DRP
- No pen test conducted
- No incident response plan
- No change management procedures
- No audit logging (security rapport L3)

Gap Table

Requirement	IKT-f. / DORA	Current State	Gap	Priority
IT security policy	IKT SS 3	Not documented	**FULL GAP**	HIGH
IT risk assessment	IKT SS 4	Security rapport exists (2026-02-12) but not a formal risk assessment	**PARTIAL**	HIGH
Access control	IKT SS 6	JWT-based, user-scoped queries. Good code-level controls. No admin access control.	**PARTIAL**	HIGH
Audit trail	IKT SS 11, DORA Art. 12	No audit logging (security rapport L3)	**FULL GAP**	HIGH

Requirement	IKT-f. / DORA	Current State	Gap	Priority
Incident management	IKT SS 8, DORA Art. 17-23	No incident response plan	**FULL GAP**	HIGH
Business continuity	IKT SS 9, DORA Art. 11	No BCP/DRP. SQLite single-file DB = single point of failure.	**FULL GAP**	HIGH
Penetration testing	IKT SS 12, DORA Art. 24-27	No pen test conducted. Security rapport is code review, not pen test.	**FULL GAP**	HIGH
Change management	IKT SS 7	No documented procedures	**FULL GAP**	MEDIUM
Third-party management	IKT SS 10, DORA Art. 28-44	Mock services only; no real third-party integrations yet. No vendor assessment framework.	**FULL GAP** for production	MEDIUM
ICT incident reporting	DORA Art. 19	No reporting capability	**FULL GAP**	MEDIUM
Register of ICT providers	DORA Art. 28(3)	Not maintained	**FULL GAP**	MEDIUM
HSTS header	Best practice	Missing (security rapport M2)	**GAP**	MEDIUM
CSP tightening	Best practice	`unsafe-inline` and `unsafe-eval` in script-src (security rapport M1)	**GAP**	MEDIUM
Distributed rate limiting	IKT SS 5	In-memory Map, resets on restart (security rapport H2)	**GAP**	HIGH
Session revocation	IKT SS 6	Table exists but unused (security rapport H1)	**GAP**	HIGH

Security Rapport Findings Impact on Compliance

Finding	Regulatory Impact
C1: Card PAN/CVV in plaintext	PCI-DSS violation; GDPR Art. 32 security adequacy failure
C2/C3: Hardcoded demo credentials	IKT-forskriften SS 5 security measures failure
C4: SHA-256 legacy passwords	GDPR Art. 32 -- inadequate cryptographic protection

Finding	Regulatory Impact
H1: No session revocation	PSD2 SCA non-compliance; IKT-forskriften SS 6 access control gap
H2: In-memory rate limiting	IKT-forskriften SS 5 -- unreliable security control
H5: Top-up without payment verification	Betalingstjenesteloven violation -- fictitious value creation
L3: No audit logging	Hvitvaskingsloven SS 30; IKT-forskriften SS 11; DORA Art. 12

---

6. Finansforetaksloven / Governance Gap Analysis

Current State

- ALAI Holding AS is registered (org.nr 932 516 136)
- No compliance officer appointed
- No formal internal control framework
- No board-level governance documented for Drop specifically

Gap Table

Requirement	Law Reference	Current State	Gap	Priority
Board competence	SS 8-4	Alem is sole director of ALAI Holding	**GAP** -- may need additional board members with financial competence	HIGH
Fit & proper documentation	SS 3-5 to 3-7	Not prepared	**FULL GAP**	HIGH
Compliance officer	SS 13-4	Not appointed	**FULL GAP**	CRITICAL
Internal control system	SS 13-2	Not documented	**FULL GAP**	HIGH
Internal audit function	SS 8-18	Not established	**FULL GAP**	MEDIUM
Risk management framework	SS 13-3	Not documented	**FULL GAP**	HIGH
Outsourcing policy	SS 13-7	Not documented	**FULL GAP**	MEDIUM
Capital adequacy plan	SS 2-9	Not prepared	**FULL GAP**	HIGH

Requirement	Law Reference	Current State	Gap	Priority
Organizational chart for license	SS 3-3	Exists in ALAI CLAUDE.md but needs formal version	**PARTIAL**	MEDIUM

---

7. Valutaregisterloven Gap Analysis

Current State

- Remittance to 6 currencies (RSD, BAM, PLN, PKR, TRY, EUR) is implemented
- Transaction records store: amount, currency, country (via recipient), date
- No SSB registration
- No reporting capability
- No purpose codes assigned

Gap Table

Requirement	Law Reference	Current State	Gap	Priority
SSB registration	SS 3	Not registered	**FULL GAP**	HIGH
Monthly reporting	SS 4, Forskrift SS 5	No reporting extract or process	**FULL GAP**	HIGH
Purpose codes	Forskrift SS 4	Not assigned to transactions	**FULL GAP**	HIGH
Country-level data	SS 5	`recipients.country` captures this	**OK**	--
Currency data	SS 5	Transaction records include currency	**OK**	--
5-year retention	SS 6	Data stored, no retention policy	**PARTIAL**	MEDIUM

Technical Gaps in Code

File: `lib/db.ts`

- `transactions` table has amount, currency, recipient_id (links to country). Good foundation.
- **Missing:** `purpose_code` column in transactions table.
- **Missing:** Reporting extract query/export function.

---

8. Consumer Protection Gap Analysis

Current State

- Landing page has `vilkar.html` (terms of service)
- Remittance shows fees and exchange rate in API response
- No framework agreement in betalingstjenesteloven format
- No Finansklagenemnda membership
- No complaint handling procedure
- No withdrawal form

Gap Table

Requirement	Law Reference	Current State	Gap	Priority
Framework agreement	Betalingstjenesteloven SS 3-1	Basic terms only	**PARTIAL** -- needs full PSD2-format agreement	HIGH
Pre-contractual information	Finansavtaleloven SS 3-23	Incomplete	**GAP**	HIGH
Fee schedule	Betalingstjenesteloven SS 3-23	Fees hardcoded in API (0.5% remittance, 1% QR). No published schedule.	**GAP**	HIGH
14-day withdrawal right	Angrerettloven SS 22	Not implemented	**FULL GAP**	HIGH
Withdrawal form	Angrerettloven SS 11	Not created	**FULL GAP**	MEDIUM
Complaint handling	Finansavtaleloven SS 3-53	No procedure	**FULL GAP**	HIGH
Finansklagenemnda membership	Finansklagenemndloven	Not member	**FULL GAP**	HIGH
Unauthorized transaction refund	Finansavtaleloven SS 4-30	No mechanism	**FULL GAP**	HIGH
Marketing substantiation	Markedsfoeringsloven SS 9	"Enklere betalinger. Lavere gebyrer." -- "Lavere gebyrer" needs substantiation if compared	**RISK**	MEDIUM

---

9. Document Inventory: What Exists vs. What Is Needed

Documents That Exist

Document	Location	Compliance Value
Terms of Service (vilkar.html)	Landing page	Partial -- needs PSD2 upgrade
Security Audit Rapport	`security/drop-security-rapport.md`	Useful for risk assessment but not a formal pen test
QA Code Quality Rapport	`project/docs/drop-qa-rapport.md`	Identifies technical debt
Architecture Document	`project/architecture/architecture-document.md`	Foundation for IT documentation
Business Case	`project/docs/zica-business-case-v2.md`	Foundation for license business plan
Feature Flags System	`lib/feature-flags.ts`	Good for controlling feature rollout
Mock Service Interfaces	`lib/services/mock-*.ts`	Defines integration requirements

Documents That Are Completely Missing

Document	Regulation	Priority
Finanstilsynet license application	Betalingstjenesteloven kap. 2	CRITICAL
AML risk assessment	Hvitvaskingsloven SS 6	CRITICAL
AML policy and procedures manual	Hvitvaskingsloven SS 8	CRITICAL
KYC procedures document	Hvitvaskingsloven SS 10-18	CRITICAL
STR reporting procedures	Hvitvaskingsloven SS 26	CRITICAL
DPIA	GDPR Art. 35	CRITICAL
Privacy policy (full, nb)	GDPR Art. 13	CRITICAL
Register of processing activities	GDPR Art. 30	HIGH
Data processing agreements	GDPR Art. 28	HIGH
SCCs for non-EEA transfers	GDPR Art. 46	HIGH
Transfer Impact Assessments	Schrems II	HIGH
IT security policy	IKT-forskriften SS 3	HIGH
Business continuity plan	IKT-forskriften SS 9	HIGH
Disaster recovery plan	IKT-forskriften SS 9	HIGH

Document	Regulation	Priority
Incident response plan	IKT-forskriften SS 8	HIGH
Framework agreement (PSD2 format)	Betalingstjenesteloven SS 3-1	HIGH
Fee schedule	Betalingstjenesteloven SS 3-23	HIGH
Complaint handling procedure	Finansavtaleloven SS 3-53	HIGH
Internal control framework	Finansforetaksloven SS 13-2	HIGH
Fit & proper documentation	Finansforetaksloven SS 3-5	HIGH
Withdrawal form	Angrerettloven SS 11	MEDIUM
Data breach response plan	GDPR Art. 33-34	HIGH
Data retention schedule	GDPR Art. 5(1)(e)	MEDIUM
Change management procedures	IKT-forskriften SS 7	MEDIUM
Capital adequacy plan	Betalingstjenesteloven SS 2-9	HIGH

---

10. Technical Gap Summary

Database Schema Gaps

The current schema (`lib/db.ts`) needs these additions for compliance:

Table/Column	Purpose	Regulation
`users.dob`	Age verification (18+)	Betalingstjenesteloven (vilkar)
`users.national_id_hash`	Fodselsnummer hash for verification	Hvitvaskingsloven SS 12
`users.risk_level`	Customer risk categorization	Hvitvaskingsloven SS 12(4)
`users.pep_status`	PEP flag	Hvitvaskingsloven SS 18
`users.sanctions_cleared`	Sanctions clearance status	Sanctions regulations
`users.kyc_method`	How KYC was performed (BankID/document/etc.)	Hvitvaskingsloven SS 12
`users.kyc_verified_at`	When KYC was completed	Hvitvaskingsloven SS 30
`transactions.purpose_code`	Valutaregister reporting	Valutaregisterloven SS 5
`audit_log` (new table)	All sensitive operations	IKT-forskriften SS 11; Hvitvaskingsloven SS 30
`aml_alerts` (new table)	Transaction monitoring alerts	Hvitvaskingsloven SS 24
`str_reports` (new table)	STR filings	Hvitvaskingsloven SS 26

Table/Column	Purpose	Regulation
`screening_results` (new table)	PEP/sanctions screening results	Hvitvaskingsloven SS 18
`consents` (new table)	GDPR consent records	GDPR Art. 7
`data_access_requests` (new table)	DSAR tracking	GDPR Art. 15-22

API Route Gaps

Route	Gap	Regulation
`POST /api/auth/register`	No age check, no BankID, no consent	PSD2, AML, GDPR
`POST /api/auth/login`	No SCA (single factor only)	PSD2 SS 4-28
`POST /api/transactions/remittance`	No pre-auth disclosure, no SCA signing, no TM hooks	PSD2, AML
`POST /api/transactions/qr-payment`	No KYC gate, no SCA signing	PSD2, AML
`POST /api/users/top-up`	No payment verification (infinite money)	PSD2 -- not a valid payment service
`POST /api/cards`	PCI-DSS violations (plaintext PAN/CVV)	PCI-DSS, GDPR Art. 32
ALL routes	No audit logging	IKT-forskriften, AML
MISSING	`GET /api/user/data-export` (DSAR)	GDPR Art. 15, 20
MISSING	`DELETE /api/user/account` (erasure)	GDPR Art. 17
MISSING	`POST /api/auth/bankid/callback`	PSD2 SCA
MISSING	`GET /api/compliance/screening/:userId`	AML SS 18
MISSING	Transaction monitoring middleware	AML SS 24

Infrastructure Gaps

Component	Current	Required	Priority
Database	SQLite (single file)	PostgreSQL or similar (HA, encryption at rest, backup)	HIGH
Rate limiting	In-memory Map	Redis/Upstash distributed limiter	HIGH
Session management	Stateless JWT only	Session table + revocation	HIGH
Audit logging	None	Immutable audit log (append-only)	HIGH
Encryption at rest	None	AES-256 for sensitive fields or full-disk	HIGH

Component	Current	Required	Priority
Backup	None	Automated daily backup with tested restore	HIGH
Monitoring	None	Application + security monitoring	HIGH
Card data	Plaintext in SQLite	Tokenized via PCI-compliant issuer (Stripe Issuing)	CRITICAL
KYC provider	Mock Sumsub	Real Sumsub/Onfido + BankID	CRITICAL
BaaS	Mock Swan	Real BaaS provider for IBAN accounts	CRITICAL

---

11. Recommended Phasing

Phase 0: Documentation Sprint (Weeks 1-4)

No code changes. Produce regulatory documents.

#	Deliverable	Owner	Weeks
1	AML risk assessment	Compliance advisor + Alem	1-2
2	AML policy and procedures	Compliance advisor	2-3
3	DPIA	Legal/Compliance advisor	2-3
4	Privacy policy (full, nb)	Legal	1-2
5	IT security policy	Tech Lead	1-2
6	Framework agreement (PSD2 format)	Legal	2-3
7	Internal control framework	Compliance advisor	2-4
8	Business plan (licensing format)	Alem + advisor	1-3

Cost estimate: Legal/compliance advisory engagement (100-200k NOK).

Phase 1: Critical Technical (Weeks 3-8)

Code changes to close critical security and compliance gaps.

#	Task	Dependency	Weeks

1	BankID integration (authentication + SCA)	BankID test agreement	3-5
2	Real KYC integration (Sumsub production)	Sumsub contract	3-5
3	Remove plaintext card storage (use Stripe Issuing or tokenization)	Stripe contract	3-4
4	Audit logging implementation	None	3-4
5	Session revocation (activate existing sessions table)	None	3-4
6	Remove top-up endpoint / integrate real payment processor	Payment partner	4-6
7	PEP/sanctions screening integration	Screening provider contract	4-6
8	Gate seed data behind NODE_ENV	None	3 (quick fix)

Phase 2: Compliance Infrastructure (Weeks 6-12)

Build compliance operational capability.

#	Task	Dependency	Weeks
1	Transaction monitoring engine (rules + alerts)	Phase 1 audit logging	6-9
2	STR filing workflow	AML procedures doc	7-10
3	Valutaregister reporting (SSB monthly extract)	SSB registration	7-10
4	DSAR endpoint (data export + erasure)	GDPR procedures	6-8
5	Consent management	GDPR procedures	6-8
6	Distributed rate limiting (Redis)	Infrastructure upgrade	6-7
7	Database migration to PostgreSQL	Infrastructure plan	8-12
8	Complaint handling system	Consumer protection docs	8-10

Phase 3: License Application (Weeks 8-16)

Submit license application with supporting documentation.

#	Task	Dependency	Weeks
1	Compile license application package	All Phase 0 documents	8-10
2	Secure initial capital (if full license)	Financial planning	8-12
3	Submit to Finanstilsynet	Complete package	10-12
4	OR: Establish agent arrangement	Partner identified	8-12
5	Finansklagenemnda membership application	Complaint handling ready	10-12
6	SSB registration	Reporting capability ready	8-10
7	Pre-launch security pen test	Phase 1-2 complete	12-16

Alternative Fast Track: Agent Model

If speed to market is critical:

1. **Weeks 1-4:** Identify and negotiate with licensed payment institution
2. **Weeks 2-6:** Complete Phase 0 documentation (still required by principal)
3. **Weeks 4-8:** Phase 1 critical technical fixes
4. **Weeks 6-10:** Agent registration by principal
5. **Week 10-12:** Soft launch under agent model
6. **Weeks 12+:** Continue Phase 2-3 in parallel, pursue own license

---

12. Risk Summary

Risk	Likelihood	Impact	Mitigation
Operating without license	CERTAIN if launched as-is	Criminal liability (betalingstjenesteloven SS 11-1), Finanstilsynet enforcement	Obtain license or agent status before first live transaction
AML non-compliance	CERTAIN if launched as-is	Criminal liability (hvitvaskingsloven SS 49), license revocation	Full AML program before launch

Risk	Likelihood	Impact	Mitigation
Data breach (plaintext card data)	HIGH given current architecture	GDPR Art. 83 fines (up to 4% of turnover or 20M EUR), reputational damage	Remove plaintext storage immediately
PSD2 SCA non-compliance	CERTAIN if launched as-is	Finanstilsynet enforcement, liability for unauthorized transactions	Implement BankID + SCA
GDPR non-compliance	HIGH if launched without DPIA	Datatilsynet fines, processing ban	Complete DPIA before any real data processing
Consumer complaint to Finansklagenemnda	MEDIUM after launch	Reputational damage, binding ruling	Join Finansklagenemnda, establish complaint handling

---

End of Drop Gap Analysis v2

Revision #6
Created 2026-02-18 08:44:34 UTC by John
Updated 2026-05-25 07:24:01 UTC by John