Compliance Overview

Drop Compliance Status

Last updated: 2026-02-13 **Source:** `legal/` directory (16 regulatory documents), `security/` directory (5 security documents), `legal/drop-gap-analysis-v2.md`, `legal/drop-regulatory-map-v2.md`

Overall Compliance Readiness: 8/100

Drop is an MVP-stage application using a **PSD2 pass-through model** (AISP reads bank balances, PISP initiates payments — Drop never holds customer money). Regulatory compliance is not expected at this stage, but documentation is being prepared. Cards are a FUTURE feature, gated behind feature flags.

Regulatory Framework

Applicable Regulations

Regulation	Norwegian Law	Relevance
PSD2	Betalingstjenesteloven (LOV-2018-11-23-85)	Core -- payment services regulation
AML/KYC	Hvitvaskingsloven (LOV-2018-06-01-23)	Core -- anti-money laundering
GDPR	Personopplysningsloven (LOV-2018-06-15-38)	Core -- personal data protection
ICT Security	IKT-forskriften / DORA	Required for financial enterprises
Financial Enterprise	Finansforetaksloven (LOV-2015-04-10-17)	Licensing and governance
Currency Registry	Valutaregisterloven	Cross-border payment reporting
Consumer Protection	Finansavtaleloven	Terms and user rights

Source: `legal/drop-regulatory-map-v2.md:1-80`

Compliance Readiness by Area

1. Licensing (0% ready)

Source: `legal/drop-gap-analysis-v2.md:31-50`

Requirement	Status	Gap
Finanstilsynet license	Not applied	FULL GAP
Client fund safeguarding	Not applicable (demo)	FULL GAP
Initial capital (20K-125K EUR)	Not secured	FULL GAP
Business plan	Exists as draft	PARTIAL
Agent arrangement	None	FULL GAP

Recommended path: Agent model under licensed PSP (1-3 months) while preparing full license application (6-12 months).

2. PSD2 / SCA (10% ready)

Source: `legal/drop-gap-analysis-v2.md:53-78`

Requirement	Status	Code Reference
Strong Customer Authentication	NOT IMPLEMENTED	No BankID, email+password only
BankID integration	NOT IMPLEMENTED	Mentioned in architecture, not in code
Dynamic linking	NOT IMPLEMENTED	No amount+payee tied to auth
Open Banking AISP/PISP	NOT IMPLEMENTED	Balance is local, not from bank
Framework agreement	PARTIAL	Landing page has `vilkar.html`
Fee transparency pre-auth	PARTIAL	Fee shown in API after submission
Session management	IMPLEMENTED	`lib/auth.ts`, `lib/middleware.ts`

3. AML/KYC (5% ready)

Requirement	Status	Gap
Customer identification	Mock only	Auto-approve KYC
Transaction monitoring	NOT IMPLEMENTED	No monitoring system

Requirement	Status	Gap
Suspicious activity reporting	NOT IMPLEMENTED	No SAR capability
Risk assessment	Document exists	`legal/risikovurdering-hvitvasking.md`
AML procedures	Document exists	`legal/hvitvaskingsrutiner.md`

4. GDPR (15% ready)

Requirement	Status	Document
Privacy notice	EXISTS (draft)	`legal/personvernerklaering.md`
DPIA	EXISTS (draft)	`legal/dpia-vurdering.md`
Terms of service	EXISTS (draft)	`legal/brukervilkar.md`
Processing register	NOT CREATED	--
DPO appointment	NOT DONE	--
Data retention policy	NOT DEFINED	--
Consent management	NOT IMPLEMENTED	--

5. ICT Security (25% ready)

Source: `security/security-rapport-2026-02-12.md:187-188`

Requirement	Status	Document/Code
Security policy	EXISTS (draft)	`legal/ikt-sikkerhetspolicy.md`
Incident handling	EXISTS (draft)	`legal/hendelseshaandtering.md`
Business continuity	EXISTS (draft)	`legal/beredskapsplan.md`
Outsourcing policy	EXISTS (draft)	`legal/utkontraktering-policy.md`
Security audit	COMPLETED	`security/drop-security-rapport.md`
Penetration testing	NOT DONE	--
Security hardening	IN PROGRESS	`security/security-hardening-implementation.md`

Security Audit Summary

Date: 2026-02-12 **Source:** `security/drop-security-rapport.md`

Before Hardening

- 4 CRITICAL, 5 HIGH, 6 MEDIUM, 4 LOW findings

After Hardening (2026-02-13)

Source: `security/security-hardening-implementation.md`

- 0 CRITICAL (all resolved)
- 0 HIGH (all resolved)
- 2 MEDIUM remaining (CSP tightening, proxy config)
- 4 LOW (acknowledged, out of scope)

Key Remediations Completed

1. **C1** -- Card data: Schema now stores only `last_four` and `token_ref` (no PAN/CVV)
2. **C2** -- Demo credentials: Gated behind `NODE_ENV !== 'production'`
3. **C4** -- SHA-256 passwords: Removed entirely, bcrypt only
4. **C6/H1** -- Session revocation: Implemented and active
5. **H4** -- Input sanitization: Applied to all text fields
6. **M5** -- Notification IDs: Validated (max 100, format check)
7. **M6** -- Settings: Currency/language validated against whitelists

---

Legal Documents Inventory

Location: `~/ALAI/products/Drop/legal/`

Document	File	Status
Privacy notice	`personvernerklaering.md`	Draft
DPIA assessment	`dpia-vurdering.md`	Draft
Terms of service	`brukervilkar.md`	Draft
AML procedures	`hvitvaskingsrutiner.md`	Draft
AML risk assessment	`risikovurdering-hvitvasking.md`	Draft
ICT security policy	`ikt-sikkerhetspolicy.md`	Draft
Incident handling	`hendelseshaandtering.md`	Draft
Business continuity	`beredskapsplan.md`	Draft
Outsourcing policy	`utkontraktering-policy.md`	Draft

Document	File	Status
Internal control	`internkontroll.md`	Draft
Suitability assessment	`egnethetsvurdering.md`	Draft
Complaint handling	`klagebehandling.md`	Draft
Licensing preparation	`konsesjonssoknad-forberedelse.md`	Draft
Business plan	`virksomhetsplan.md`	Draft
Gap analysis v2	`drop-gap-analysis-v2.md`	Complete
Regulatory map v2	`drop-regulatory-map-v2.md`	Complete

Security Documents Inventory

Location: `~/ALAI/products/Drop/security/`

Document	File	Status
Security audit rapport	`drop-security-rapport.md`	Complete (2026-02-12)
Gap analysis	`gap-analysis.md`	Complete (2026-02-12)
Hardening checklist	`hardening-checklist.md`	In progress
Hardening implementation	`security-hardening-implementation.md`	Complete (2026-02-13)
Formal assessment	`security-rapport-2026-02-12.md`	Complete (2026-02-12)

Remediation Phases

Phase 1 -- Current Sprint (in progress)

Security fixes, architecture cleanup, test suite, CI/CD.

Phase 2 -- Banking Integration (pending partner selection)

BankID, Open Banking AISP/PISP, real KYC, PostgreSQL migration.

Phase 3 -- Production Launch (after Phase 2 + follow-up audit)

Audit logging, error handling, monitoring, staging environment, load testing, external penetration test.

Source: `security/security-rapport-2026-02-12.md:196-220`

Revision #10
Created 2026-02-23 11:29:00 UTC by John
Updated 2026-07-12 20:00:41 UTC by John