Regulatory Map

Drop Regulatory Map v2

Norwegian Financial Services Regulatory Framework

Date: 2026-02-12 **Prepared for:** ALAI Holding AS / Drop Payment App **Scope:** All regulations applicable to a payment app serving ALL residents of Scandinavia **App model:** Pass-through payments (remittance + QR in-store), no deposit-taking

---

Table of Contents

---

1. Finanstilsynet Licensing

Applicable Law

- **Finanstilsynsloven** (Lov om Finanstilsynet, LOV-1956-12-07-1)
- **Betalingstjenesteloven** kapittel 2 (licensing provisions)
- **Finansforetaksloven** (LOV-2015-04-10-17) for broader financial enterprise requirements

License Options for Drop

Option A: Begrenset betalingsforetak (Limited Payment Institution)

Law: Betalingstjenesteloven (LOV-2018-11-23-85) SS 2-10c

Requirement	Detail
Monthly transaction volume	Max 6 million NOK/month average over 12 months
Capital requirement	None (simplified regime)
Application	Simplified application to Finanstilsynet
Passporting	NO -- Norway only, no EEA passport
Fit & proper	Directors and beneficial owners must pass fit & proper assessment
AML	Full AML compliance still required
PSD2 SCA	Required
Safeguarding	Client funds must be safeguarded (segregated account or insurance)

Pros: Faster to obtain (3-6 months), lower capital cost, suitable for MVP launch. **Cons:** Volume ceiling, no passporting to Sweden/Denmark, must upgrade if volume exceeds threshold.

Drop fit: Good for initial launch. 6M NOK/month allows approximately 3,000 remittances of 2,000 NOK average.

Option B: Ordinaert betalingsforetak (Full Payment Institution)

Law: Betalingstjenesteloven SS 2-3 to SS 2-10

Requirement	Detail
Initial capital	125,000 EUR (approx. 1.4M NOK) for payment services incl. money remittance
Ongoing capital	Higher of: initial capital, OR calculated based on method A/B/C in SS 2-9
Application timeline	6-12 months (Finanstilsynet review)
Passporting	YES -- EEA-wide via notification to host state supervisors
Governance	Board, compliance officer, internal audit function

Requirement	Detail
Safeguarding	Client funds in segregated account OR insurance/guarantee
Fit & proper	All board members, CEO, compliance officers
Reporting	Annual reports, quarterly capital adequacy, incident reports

Pros: No volume limit, EEA passporting to Sweden/Denmark, full credibility. **Cons:** Higher capital, longer timeline, heavier governance burden.

Drop fit: Target license for scaling to all of Scandinavia. Apply after MVP validates market.

Option C: Agent Model (under existing licensee)

Law: Betalingstjenesteloven SS 2-12

Requirement	Detail
Concept	Drop operates as agent of an existing licensed payment institution
Registration	The principal (licensee) registers Drop as agent with Finanstilsynet
Capital	None required from Drop -- principal is responsible
AML	Principal's AML program applies; Drop must comply operationally
Liability	Principal is liable for Drop's actions
Speed	Fastest route to market (1-3 months)

Pros: Fastest launch, no capital requirement, leverage existing compliance infrastructure. **Cons:** Revenue share with principal, less control, dependent on partner's license scope.

Potential partners for agent model:

- Licensed Norwegian payment institutions (e.g., smaller PSPs)
- Licensed EMIs operating in Norway via passporting
- BaaS providers (Swan, Modulr, Banking Circle) with appropriate licenses

Required Documents for Licensing Application

1. Business plan with 3-year financial projections
2. Description of payment services to be offered (SS 2-4)
3. Organizational chart with fit & proper documentation for all key persons
4. AML/CFT policy and procedures (full program)

5. Operational procedures and internal control description
6. IT security policy and business continuity plan
7. Client fund safeguarding arrangements
8. Capital adequacy calculations and evidence of initial capital
9. Outsourcing policy (if using third-party services)
10. Complaint handling procedures

Priority: CRITICAL -- Must be resolved before any live transaction

---

2. Betalingstjenesteloven / PSD2

Applicable Law

- **Betalingstjenesteloven** (LOV-2018-11-23-85) -- Norwegian implementation of PSD2
- **Betalingssystemloven** (LOV-1999-12-17-95) -- Payment systems
- **Forskrift om betalingstjenester** (FOR-2019-02-15-152) -- Regulation on payment services

Strong Customer Authentication (SCA)

Law: Betalingstjenesteloven SS 4-28, SS 4-29; Delegated Regulation (EU) 2018/389

Requirement	Section	What Drop Must Do
SCA for electronic payments	SS 4-28	Apply SCA for all payment initiation and online access
Two of three factors	Art. 6-8 (Del. Reg.)	Combine: knowledge (PIN/password), possession (phone/device), inherence (biometrics)
Dynamic linking	Art. 5 (Del. Reg.)	Transaction amount and payee must be linked to authentication code
Exemptions	Art. 10-18 (Del. Reg.)	Low-value transactions (<500 NOK contactless), trusted beneficiaries, recurring payments
90-day re-authentication	Art. 10 (Del. Reg.)	Re-authenticate if account not accessed for 90 days

Current state: Drop uses email+password login with JWT. BankID is mentioned but not implemented. No SCA compliance.

Required implementation:

1. BankID integration for initial authentication (covers possession + knowledge)
2. Transaction signing with BankID or app-based second factor for payments
3. Dynamic linking: display amount + payee in BankID signing dialog
4. Session timeout and re-authentication after 5 minutes of inactivity (for payment sessions)

Open Banking (PSD2 Access to Account)

Law: Betalingstjenesteloven SS 4-40 to SS 4-46

Requirement	Section	Relevance to Drop
AISP (Account Information)	SS 4-41	If Drop reads user bank balances via Open Banking
PISP (Payment Initiation)	SS 4-44	If Drop initiates transfers from user bank accounts
Dedicated interface (API)	SS 4-40	Drop must use banks' PSD2 APIs
PSU consent	SS 4-41(2)	Explicit user consent required before accessing accounts
No storing of credentials	SS 4-44(3)	Drop must NOT store user's bank login credentials

Architecture note: Drop's stated pass-through model relies on Open Banking. This requires either AISP/PISP license or agent arrangement with a licensed AISP/PISP.

Consumer Protection (PSD2)

Law: Betalingstjenesteloven kapittel 3 and 4

Requirement	Section	What Drop Must Do
Pre-contractual information	SS 3-1 to SS 3-8	Provide framework agreement with all fees, exchange rates, execution time
Information per transaction	SS 3-22 to SS 3-26	Receipt with amount, fees, exchange rate, reference, date
Execution time	SS 4-15	Remittance: must credit recipient's PSP by end of next business day (EEA), D+4 for non-EEA
Refund rights	SS 4-19 to SS 4-22	Unauthorized transactions: user liable max 450 NOK if negligent, full refund if not
Value date	SS 4-18	Credit value date = date amount received by recipient's PSP

Requirement	Section	What Drop Must Do
Charges transparency	SS 3-23	All charges must be disclosed BEFORE transaction is authorized
Exchange rate	SS 3-24	Actual exchange rate and reference rate must be disclosed

Required documents:

1. Framework agreement / user terms (rammeavtale)
2. Fee schedule (gebyroppstilling)
3. Transaction receipts (per transaction)
4. Pre-authorization disclosure (amount, fees, FX rate, ETA)

Priority: CRITICAL -- PSD2 is the legal basis for operating

---

3. Hvitvaskingsloven / AML

Applicable Law

- **Hvitvaskingsloven** (LOV-2018-06-01-23) -- Anti-Money Laundering Act
- **Hvitvaskingsforskriften** (FOR-2018-09-14-1324) -- AML Regulation
- **Sanksjonsforskrifter** -- Various sanctions regulations

Customer Due Diligence (KYC)

Law: Hvitvaskingsloven SS 10 to SS 18

Requirement	Section	What Drop Must Do
Identity verification	SS 12	Verify name, DOB, national ID number (fodselsnummer) using valid ID document
Electronic verification	SS 12(3)	BankID qualifies as electronic verification for Norwegian residents
Beneficial owner (individuals)	SS 13	For individual customers: the customer themselves
Purpose of relationship	SS 12(1)d	Document why the customer is using the service

Requirement	Section	What Drop Must Do
Ongoing monitoring	SS 24	Monitor transactions for unusual patterns
Enhanced due diligence	SS 17-18	Required for higher-risk customers, countries, or transaction patterns
Simplified due diligence	SS 16	Possible for lower-risk, low-value services (not recommended for remittance)
Record keeping	SS 30	Store KYC data for 5 years after relationship ends
Re-verification	SS 24(3)	When risk profile changes or doubts about existing data

Current state: Drop has a `kyc_status` field (pending/approved/rejected) and mock Sumsub integration. No real KYC implementation.

Required implementation:

1. BankID integration for Norwegian residents (covers identity verification)
2. ID document verification for non-BankID eligible (passport/national ID via Sumsub/Onfido)
3. Address verification (e.g., Folkeregisteret lookup or utility bill)
4. Source of funds declaration for transfers above thresholds
5. Risk categorization per customer (low/medium/high)

Transaction Monitoring

Law: Hvitvaskingsloven SS 24, SS 25

Requirement	Section	What Drop Must Do
Ongoing monitoring	SS 24	Automated monitoring of all transactions
Unusual transactions	SS 25	Investigate transactions inconsistent with customer profile
STR filing	SS 26	File Suspicious Transaction Reports with EFE (Ekonomisk kriminalitet enheten)
No tipping off	SS 28	NEVER inform the customer that an STR has been filed
Internal procedures	SS 8	Written AML procedures, appointed AML officer
Training	SS 36	Regular AML training for all relevant staff

Transaction monitoring rules to implement:

1. Structuring detection (multiple transactions just below reporting thresholds)
2. Rapid movement (funds in/out within short timeframe)
3. Unusual corridors (sudden changes in destination countries)
4. Volume spikes (significantly above normal pattern)
5. High-risk country flags (FATF grey/black list countries)
6. PEP matching (see below)

PEP and Sanctions Screening

Law: Hvitvaskingsloven SS 18; Various sanctions forskrifter

Requirement	Section	What Drop Must Do
PEP screening	SS 18(1)	Screen all customers against PEP lists at onboarding and ongoing
Enhanced due diligence for PEPs	SS 18(2-3)	Senior management approval, source of wealth, enhanced monitoring
Sanctions screening	Sanctions regulations	Screen against UN, EU, and Norwegian sanctions lists
Ongoing screening	SS 18(5), SS 24	Continuous monitoring, not just onboarding
Close associates	SS 18(1)b	Screen family members and known close associates of PEPs

Required integrations:

1. PEP database (ComplyAdvantage, Refinitiv World-Check, or similar)
2. Sanctions list screening (EU consolidated list, UN Security Council list, Norwegian MFA list)
3. Ongoing batch screening (daily or real-time for new entries)

AML Risk Assessment

Law: Hvitvaskingsloven SS 6, SS 7

Drop must conduct and document a risk assessment covering:

Risk Factor	Assessment for Drop
Customer risk	General population of Scandinavia; some customer segments may be higher-risk based on occupation or source of funds
Product/service risk	Remittance services are inherently higher-risk (FATF typology); QR payments are lower-risk

Risk Factor	Assessment for Drop
Channel risk	Mobile/digital-only = moderate risk (no face-to-face)
Geographic risk	Corridors to 30+ countries, some high-risk jurisdictions. Turkey, Pakistan on FATF monitoring. Serbia, Bosnia lower-risk but outside EU
Transaction risk	Variable amounts, cross-border nature

Required documents:

1. Enterprise-wide AML risk assessment (virksomhetsrettet risikovurdering)
2. AML policy and procedures manual (AML-handbok)
3. STR reporting procedures
4. Customer risk categorization model
5. Training plan and records
6. AML officer appointment letter

Priority: CRITICAL -- Operating without AML compliance is a criminal offense (SS 49)

---

4. Personopplysningsloven / GDPR

Applicable Law

- **Personopplysningsloven** (LOV-2018-06-15-38) -- Norwegian implementation of GDPR
- **GDPR** (Regulation (EU) 2016/679) -- Incorporated via EEA Agreement
- **Forskrift om behandling av personopplysninger** (FOR-2018-06-15-876)

Data Processing Requirements

Requirement	GDPR Article	What Drop Must Do
Lawful basis	Art. 6	Contract performance (Art. 6(1)(b)) for core service; Legal obligation (Art. 6(1)(c)) for AML; Consent (Art. 6(1)(a)) for marketing
Special category data	Art. 9	Avoid processing unless necessary; biometric data for KYC requires explicit consent or legal obligation

Requirement	GDPR Article	What Drop Must Do
Transparency	Art. 13-14	Privacy policy in Norwegian (nb), covering all processing activities
Purpose limitation	Art. 5(1)(b)	Only process for stated purposes
Data minimization	Art. 5(1)(c)	Collect only what is necessary
Storage limitation	Art. 5(1)(e)	Define retention periods (AML: 5 years; transactions: 5 years; marketing: until consent withdrawn)
Accuracy	Art. 5(1)(d)	Keep data up to date; allow corrections
Data subject rights	Art. 15-22	Access, rectification, erasure, portability, restriction, objection
Records of processing	Art. 30	Maintain a Register of Processing Activities (behandlingsprotokoll)

DPIA (Data Protection Impact Assessment)

GDPR Article 35; Datatilsynet guidelines

A DPIA is MANDATORY for Drop because:

1. Processing of financial data at scale
2. Systematic monitoring of individuals (transaction monitoring)
3. Cross-border data transfers (remittance to 30+ countries)
4. Vulnerable groups potential (newly arrived residents, etc.)
5. New technology use (mobile payments, QR)

DPIA Requirement	What Drop Must Document
Processing description	All personal data flows in the app
Necessity and proportionality	Why each data element is needed
Risk assessment	Risks to data subjects from processing
Mitigating measures	Technical and organizational safeguards
Datatilsynet consultation	Required if residual risk remains high after mitigations (Art. 36)

Cross-Border Transfers

GDPR Chapter V (Art. 44-49)

Destination	Transfer Mechanism Required

EEA countries	No restriction (free flow)
Adequacy decision countries (UK, Japan, etc.)	No additional safeguard needed
Serbia	No adequacy decision -- needs SCCs (Standard Contractual Clauses) + TIA
Bosnia & Herzegovina	No adequacy decision -- needs SCCs + TIA
Turkey	No adequacy decision -- needs SCCs + TIA
Pakistan	No adequacy decision -- needs SCCs + TIA; higher supplementary measures
Poland	EEA member -- no restriction

Transfer Impact Assessment (TIA): Required for each non-adequate country. Must assess local surveillance laws and determine if SCCs provide sufficient protection.

Required Documents

1. Privacy policy (personvernerklaering) -- Norwegian language
2. DPIA (vurdering av personvernkonsekvenser)
3. Register of processing activities (behandlingsprotokoll)
4. Data processing agreements (databehandleravtale) with all processors
5. Standard Contractual Clauses for non-EEA transfers
6. Transfer Impact Assessments per destination country
7. Cookie/consent management policy
8. Data breach response plan (bruddhandteringsplan)
9. Data subject rights procedures (innsynsprosedyre)
10. Data retention schedule (lagringstidsplan)

Priority: HIGH -- Must be in place before processing any personal data

---

5. IKT-forskriften / DORA

Applicable Law

- **IKT-forskriften** (FOR-2003-05-21-630) -- Current IT security regulation for financial institutions
- **DORA** (Regulation (EU) 2022/2554) -- Digital Operational Resilience Act

- **Proposed Norwegian DORA implementation** -- Expected via amendment to Finanstilsynsloven or separate act

Current IKT-forskriften Requirements

Requirement	Section	What Drop Must Do
IT strategy	SS 3	Document IT strategy aligned with business strategy
Risk assessment	SS 4	IT risk assessment, updated annually
Security measures	SS 5	Technical and organizational security controls
Access control	SS 6	Role-based access, principle of least privilege
Change management	SS 7	Documented procedures for system changes
Incident management	SS 8	Incident detection, response, reporting to Finanstilsynet
Business continuity	SS 9	BCP/DRP with regular testing
Outsourcing	SS 10	Due diligence on IT outsourcing partners
Audit trail	SS 11	Logging of all significant events
Testing	SS 12	Regular security testing (pen tests, vulnerability scans)

DORA Requirements (coming for Norway)

Regulation (EU) 2022/2554 -- Applies to payment institutions

DORA Requirement	Article	What Drop Must Do
ICT risk management framework	Art. 5-16	Comprehensive ICT risk management framework
ICT incident management	Art. 17-23	Classify, manage, report ICT incidents
Major incident reporting	Art. 19	Report to Finanstilsynet within 4 hours (initial), 72 hours (intermediate), 1 month (final)
Digital operational resilience testing	Art. 24-27	Regular testing including TLPT (threat-led penetration testing) for significant entities
Third-party risk management	Art. 28-44	Contractual requirements for ICT service providers

DORA Requirement	Article	What Drop Must Do
Register of ICT providers	Art. 28(3)	Maintain register of all third-party ICT providers
Information sharing	Art. 45	Participate in threat intelligence sharing

Required Documents

1. IT security policy (IKT-sikkerhetspolicy)
2. IT risk assessment (IKT-risikovurdering)
3. Business continuity plan (beredskapsplan)
4. Disaster recovery plan (katastrofegjenopprettingsplan)
5. Incident response plan (hendelseshandteringsplan)
6. Change management procedures
7. Access control policy
8. Third-party/outsourcing assessment register
9. Penetration test reports (annual minimum)
10. Vulnerability scan reports (quarterly minimum)

Priority: HIGH -- Required for license application and ongoing compliance

---

6. Finansforetaksloven

Applicable Law

- **Finansforetaksloven** (LOV-2015-04-10-17) -- Financial Enterprises Act
- Applies to payment institutions via betalingstjenesteloven SS 2-7 cross-references

Governance Requirements

Requirement	Section	What Drop Must Do
Board composition	SS 8-4	Board with adequate competence, independent members recommended
CEO/management	SS 8-7	Appointed CEO with fit & proper documentation

Requirement	Section	What Drop Must Do
Fit & proper	SS 3-5 to SS 3-7	All board members and senior management: police certificate, CV, qualifications assessment
Internal control	SS 13-2	Internal control system, compliance function
Compliance officer	SS 13-4	Designated compliance officer
Internal audit	SS 8-18	Internal audit function (can be outsourced for smaller institutions)
Risk management	SS 13-3	Risk management framework proportionate to size
Outsourcing	SS 13-7	Notification to Finanstilsynet for material outsourcing
Reporting	SS 14-1	Regular reporting to Finanstilsynet (annual accounts, etc.)

Capital Requirements

License Type	Initial Capital	Ongoing Capital
Begrenset betalingsforetak	None specified (simplified)	Must have adequate resources
Ordinaert betalingsforetak (money remittance)	20,000 EUR	Method A/B/C calculation or initial capital, whichever higher
Ordinaert betalingsforetak (payment services broader)	125,000 EUR	Method A/B/C calculation or initial capital, whichever higher

Note: Drop's combined remittance + QR payment services likely falls under the 125,000 EUR tier.

Required Documents

1. Articles of association (vedtekter)
2. Board member CVs and fit & proper declarations
3. Police certificates for board/management
4. Organizational chart with reporting lines
5. Internal control framework description
6. Compliance function description
7. Risk management policy
8. Capital adequacy plan

Priority: CRITICAL -- Required for license application

7. Valutaregisterloven

Applicable Law

- **Valutaregisterloven** (LOV-2004-12-17-109) -- Foreign Exchange Register Act
- **Valutaregisterforskriften** (FOR-2005-02-10-121) -- Foreign Exchange Register Regulation

Cross-Border Reporting Requirements

Requirement	Section	What Drop Must Do
Registration	SS 3	Register as reporting entity with Statistisk sentralbyra (SSB)
Reporting obligation	SS 4	Report all cross-border payment transactions
Transaction data	SS 5	Report: amount, currency, country, payer/payee, purpose code
Threshold	Forskriften SS 4	All cross-border transactions must be reported (no minimum threshold for payment institutions)
Reporting frequency	Forskriften SS 5	Monthly electronic reporting to SSB
Data retention	SS 6	5 years
Large cash transactions	SS 4a	Not applicable (Drop is digital-only)

Implementation requirements:

1. Assign purpose codes (SWIFT MT103 / ISO 20022 purpose codes) to all remittances
2. Collect destination country per transaction (already in DB schema: `recipients.country`)
3. Build monthly reporting extract for SSB
4. Register with SSB as reporting entity

Required Documents

1. SSB registration as valutaregisterpliktig
2. Monthly reporting procedures
3. Purpose code mapping for transaction types
4. Reporting archive (5-year retention)

Priority: HIGH -- Must be in place before first cross-border transaction

8. Consumer Protection

Applicable Law

- **Angrerettloven** (LOV-2014-06-20-27) -- Right of Withdrawal Act (distance selling)
- **Finansavtaleloven** (LOV-2020-12-18-146) -- Financial Contracts Act (replaces 1999 version, effective 2023)
- **Markedsfoeringsloven** (LOV-2009-01-09-2) -- Marketing Act
- **Finansklagenemnda** -- Financial Complaints Board (external dispute resolution)

Angrerettloven (Right of Withdrawal)

Sections relevant to financial services:

Requirement	Section	What Drop Must Do
Right of withdrawal	SS 22	14-day withdrawal right for framework agreement (user registration)
Exception for executed transactions	SS 22(2)g	No withdrawal right for fully executed payment transactions
Pre-contractual information	SS 8	Provide all required information before contract conclusion
Withdrawal form	SS 11	Provide standard withdrawal form
Confirmation	SS 9	Written confirmation of agreement on durable medium

Finansavtaleloven (Financial Contracts Act)

New version effective 2023 -- significant consumer protection enhancements

Requirement	Section	What Drop Must Do
Duty to advise	SS 3-1	Assess customer needs before recommending services
Pre-contractual information	SS 3-23 to SS 3-38	Extensive pre-contractual disclosure requirements

Requirement	Section	What Drop Must Do
Framework agreement	SS 4-1	Written framework agreement for recurring payment services
Unauthorized transactions	SS 4-30	Refund unauthorized transactions immediately (max 450 NOK customer liability if negligent)
Misdirected payments	SS 4-33	Assist in recovering misdirected payments
Complaint handling	SS 3-53	Internal complaint handling procedure, respond within 15 business days
Fee transparency	SS 3-25	All fees disclosed upfront in standardized format
Exchange rate disclosure	SS 3-34	Actual rate + reference rate + markup disclosed before transaction
Execution time	SS 4-12	Payment execution times must be disclosed and adhered to

Finansklagenemnda (Financial Complaints Board)

Law: Finansklagenemndloven (LOV-2016-06-17-29)

Requirement	Detail
Membership	Mandatory for all financial service providers in Norway
Cost	Annual membership fee based on number of complaints
Compliance	Must comply with Finansklagenemnda decisions
Information	Must inform customers about right to complain to Finansklagenemnda

Markedsfoeringsloven (Marketing)

Requirement	Section	What Drop Must Do
No misleading marketing	SS 6-8	Do not overstate benefits or understate costs/risks
Price information	SS 10	Clear, accurate pricing in all marketing
Comparison claims	SS 9	Substantiate any claims of being "cheaper than Vipps"

Requirement	Section	What Drop Must Do
Spam/electronic marketing	SS 15	Opt-in consent required for electronic marketing

Required Documents

1. Framework agreement (rammeavtale) with all financial terms
2. Fee schedule (gebyrliste) in standardized format
3. Withdrawal form (angrerettskjema)
4. Internal complaint handling procedure (klageprosedyre)
5. Finansklagenemnda membership registration
6. Privacy-compliant marketing consent mechanism

Priority: HIGH -- Consumer protection failure leads to Finanstilsynet enforcement and reputational damage

---

9. DORA Timeline for Norway

Background

DORA (Digital Operational Resilience Act, Regulation (EU) 2022/2554) applies in the EU from **17 January 2025**. Norway, as an EEA member, must incorporate DORA via the EEA Agreement.

Expected Timeline

Date	Milestone
17 Jan 2025	DORA applicable in EU
2025 Q1-Q2	EEA Joint Committee decision to incorporate DORA into EEA Agreement (ongoing)
2025 H2 - 2026 H1	Norwegian legislative process (Prop. to Stortinget)
2026 H2 (estimated)	Norwegian DORA implementation enters force
2026-2027	Transition period for Norwegian financial entities

Current Status (February 2026)

- EU DORA has been applicable since January 2025
- The Norwegian government has proposed incorporation into the EEA Agreement
- Finanstilsynet has communicated expectations that Norwegian firms prepare for DORA
- The existing IKT-forskriften remains in force and is substantially aligned with DORA, but DORA adds:
  - More prescriptive ICT incident reporting (4h/72h/1mo)
  - Threat-Led Penetration Testing (TLPT) for significant entities
  - Third-party ICT provider oversight framework
  - Information sharing requirements

Practical Implication for Drop

- **Now:** Comply with IKT-forskriften (current regulation)
- **2026 H2:** Expect DORA requirements to apply
- **Strategy:** Build ICT risk management framework aligned with DORA from the start, so no retrofit is needed
- Payment institutions are explicitly within DORA scope (Art. 2(1)(d))

---

10. Regulatory Priority Matrix

Phase 1: Pre-Launch (Must-Have for First Transaction)

#	Regulation	Key Action	Documents
1	License	Apply for begrenset betalingsforetak OR establish agent arrangement	Application package
2	AML	Full AML program: risk assessment, KYC procedures, STR process	AML handbook, risk assessment
3	PSD2	SCA implementation (BankID), framework agreement, fee disclosure	Rammeavtale, gebyrliste
4	GDPR	DPIA, privacy policy, processing register	DPIA, personvernerklaering

#	Regulation	Key Action	Documents
5	Governance	Fit & proper, compliance officer, internal control	Board docs, compliance framework

Phase 2: Launch + 6 Months

#	Regulation	Key Action	Documents
6	Valutaregisteret	Register with SSB, establish monthly reporting	SSB registration, reporting procedures
7	IKT-forskriften	IT security policy, BCP, pen test	IKT policy, BCP, test reports
8	Consumer protection	Finansklagenemnda membership, complaint handling	Membership, klageprosedyre
9	AML ongoing	Transaction monitoring system, PEP/sanctions screening	TM rules, screening integration
10	Capital	Secure initial capital if pursuing ordinaert license	Capital evidence

Phase 3: Scaling (12+ Months)

#	Regulation	Key Action	Documents
11	License upgrade	Apply for ordinaert betalingsforetak for Scandinavia expansion	Full application
12	DORA	Full DORA compliance (incident reporting, TLPT, third-party oversight)	DORA compliance framework
13	Passporting	Notify host state supervisors (Finansinspektionen SE, Finanstilsynet DK)	Passporting notification
14	PCI-DSS	If issuing/processing cards: PCI-DSS certification	SAQ/ROC depending on volume

---

Summary: Required Document Inventory

#	Document	Regulation	Priority
1	License application package	Betalingstjenesteloven	CRITICAL
2	AML risk assessment	Hvitvaskingsloven SS 6	CRITICAL
3	AML policy and procedures	Hvitvaskingsloven SS 8	CRITICAL
4	KYC procedures	Hvitvaskingsloven SS 10-18	CRITICAL
5	STR reporting procedures	Hvitvaskingsloven SS 26	CRITICAL
6	Framework agreement (rammeavtale)	Betalingstjenesteloven SS 3-1	CRITICAL
7	Fee schedule	Betalingstjenesteloven SS 3-23	CRITICAL
8	Privacy policy	GDPR Art. 13	CRITICAL
9	DPIA	GDPR Art. 35	CRITICAL
10	Register of processing activities	GDPR Art. 30	HIGH
11	Data processing agreements	GDPR Art. 28	HIGH
12	Standard Contractual Clauses (non-EEA transfers)	GDPR Art. 46	HIGH
13	Transfer Impact Assessments	GDPR Schrems II	HIGH
14	IT security policy	IKT-forskriften SS 3	HIGH
15	Business continuity plan	IKT-forskriften SS 9	HIGH
16	Incident response plan	IKT-forskriften SS 8	HIGH
17	Internal control framework	Finansforetaksloven SS 13-2	HIGH
18	Fit & proper documentation	Finansforetaksloven SS 3-5	HIGH
19	Complaint handling procedure	Finansavtaleloven SS 3-53	HIGH
20	Withdrawal form	Angrerettloven SS 11	HIGH
21	SSB registration and reporting	Valutaregisterloven SS 3	HIGH
22	Third-party outsourcing register	DORA Art. 28	MEDIUM
23	Penetration test reports	IKT-forskriften SS 12	MEDIUM
24	AML training records	Hvitvaskingsloven SS 36	MEDIUM
25	Data retention schedule	GDPR Art. 5(1)(e)	MEDIUM

End of Drop Regulatory Map v2

Revision #7
Created 2026-02-18 08:44:34 UTC by John
Updated 2026-05-25 07:23:59 UTC by John