KYC & AML Flow

KYC/AML Flow -- Low-Level Design

Document: LLD-KYC-AML **Status:** Approved **Last updated:** 2026-02-21 **Author:** Standards Architect **Applies to:** Drop v1.0 (PSD2 pass-through model) **Regulatory basis:** Hvitvaskingsloven (LOV-2018-06-01-23), GDPR (Personopplysningsloven)

Overview

Drop's KYC (Know Your Customer) and AML (Anti-Money Laundering) system ensures compliance with Norwegian anti-money laundering law (hvitvaskingsloven). The system has three phases:

1. **Onboarding KYC** -- Identity verification at registration via BankID + Sumsub document verification
2. **Transaction monitoring** -- Real-time and periodic analysis of transaction patterns
3. **Ongoing due diligence** -- Periodic re-screening of PEP/sanctions lists and adverse media

Drop uses a risk-based approach per hvitvaskingsloven section 4-6: higher-risk customers and transactions receive enhanced scrutiny.

KYC Verification Flow

```
sequenceDiagram
    participant User
    participant Drop as Drop API
    participant BankID
    participant Sumsub
    participant DB as PostgreSQL

    Note over User,DB: Phase 1 -- BankID Identity Verification
```

```
User->>Drop: Login via BankID OIDC
Drop->>BankID: Exchange auth code for ID token
BankID->>Drop: ID token (pid, name, DOB)
Drop->>Drop: Parse pid (fodselsnummer)
Drop->>Drop: Verify age >= 18
Drop->>Drop: Hash pid with SHA-256
Drop->>DB: Find/create user (national_id_hash)
Drop->>DB: Set kyc_status = 'approved', kyc_method = 'bankid'

Note over User,DB: Phase 2 -- Sumsub Enhanced Verification
Drop->>Sumsub: Create applicant (user_id, name, DOB)
Sumsub->>Drop: applicant_id
Drop->>DB: Store applicant_id in users table
Drop->>User: Request document upload (if EDD triggered)

alt Standard CDD (low risk)
    Note over User,Sumsub: BankID sufficient -- no document upload
    Sumsub->>Sumsub: Auto-approve based on BankID data
else Enhanced CDD (high risk)
    User->>Sumsub: Upload ID document + selfie
    Sumsub->>Sumsub: Document verification + liveness check
end

Note over User,DB: Phase 3 -- PEP/Sanctions Screening
Sumsub->>Sumsub: Screen against PEP lists
Sumsub->>Sumsub: Screen against sanctions (OFAC, UN, EU, Norway)
Sumsub->>Sumsub: Screen adverse media

Sumsub->>Drop: Webhook: verification result
Drop->>DB: Update kyc_status (approved/rejected)
Drop->>DB: Insert screening_results (pep, sanctions, adverse_media)
Drop->>DB: Update users.risk_level, pep_status, sanctions_cleared

alt Screening match found
    Drop->>DB: Create aml_alert (severity based on match type)
    Drop->>Drop: Block user from transactions
end
```

KYC Applicant States

```
stateDiagram-v2
    [*] --> bankid_verified : BankID login successful
    bankid_verified --> sumsub_pending : Sumsub applicant created
    sumsub_pending --> document_requested : EDD required (high risk)
    sumsub_pending --> screening : CDD sufficient (low risk)
    document_requested --> document_uploaded : User uploads ID + selfie
    document_uploaded --> document_review : Sumsub processes documents
    document_review --> screening : Documents verified
    document_review --> document_rejected : Documents invalid
    document_rejected --> document_requested : User retries
    screening --> approved : All clear (PEP, sanctions, media)
    screening --> manual_review : Potential match found
    manual_review --> approved : Compliance officer clears
    manual_review --> rejected : Confirmed match or fraud
    approved --> ongoing_monitoring : Periodic re-screening
    ongoing_monitoring --> manual_review : Re-screening match
    ongoing_monitoring --> approved : Re-screening clear
    rejected --> [*]
```

Document Verification Steps

When Enhanced Due Diligence (EDD) is triggered, Sumsub performs multi-step document verification:

Step	Check	Provider	Pass Criteria
1. Document quality	Image clarity, glare, blur	Sumsub AI	Readable text, clear photo
2. Document authenticity	Hologram detection, font analysis, template matching	Sumsub AI	Matches known document templates
3. Data extraction	OCR: name, DOB, document number, expiry	Sumsub OCR	All fields extracted successfully
4. Cross-reference	Extracted data vs BankID data (name, DOB)	Drop API	Name and DOB match within tolerance
5. Liveness check	Selfie vs document photo, anti-spoofing	Sumsub AI	Face match > 80%, liveness confirmed
6. Expiry check	Document expiration date	Sumsub	Document not expired

Accepted documents (Norway-specific):

- Norwegian passport (preferred)
- Norwegian national ID card
- Norwegian driver's license (with photo)
- EEA passport or national ID card (for EEA residents)

PEP/Sanctions Screening

Screening Sources

List	Source	Update Frequency	Scope
Norwegian PEP list	Finanstilsynet	Real-time	Norwegian politically exposed persons
OFAC SDN	US Treasury	Daily	Global sanctions
UN Consolidated	UN Security Council	Real-time	Global sanctions
EU Consolidated	European Commission	Daily	EU sanctions
Norwegian sanctions	Utenriksdepartementet	As published	Norway-specific restrictions
Adverse media	Sumsub media monitoring	Continuous	Negative news, legal proceedings

Screening Triggers

Trigger	Type	Screening Scope
New user registration	Initial CDD	Full: PEP + sanctions + adverse media
Transaction > 10,000 NOK	Transaction monitoring	Sanctions only (real-time)
Cumulative 30-day > 50,000 NOK	Periodic monitoring	Full re-screening
Quarterly schedule	Ongoing due diligence	Full re-screening of all active users
User data change	Event-driven	Full re-screening

Database: `screening_results` table

Column	Type	Values
`screening_type`	TEXT	`pep`, `sanctions`, `adverse_media`

Column	Type	Values
`provider`	TEXT	`sumsub` (or future: `refinitiv`, `dow_jones`)
`result`	TEXT	`clear`, `match`, `potential_match`, `error`
`match_details`	TEXT (JSON)	Match metadata (name similarity, list source, entry details)

Risk Scoring Algorithm

Drop assigns a risk level to each user based on multiple factors. The risk score determines the level of due diligence applied.

Risk Factor Matrix

Factor	Low Risk (1 pt)	Medium Risk (3 pts)	High Risk (5 pts)
Country of origin	Norway, Sweden, Denmark, Finland	EU/EEA countries	Non-EEA, high-risk jurisdictions (FATF grey/black list)
Remittance corridor	SEPA (intra-EEA)	Non-EEA low-risk	Pakistan, Turkey, non-EEA high-risk
Transaction volume (30-day)	< 10,000 NOK	10,000-50,000 NOK	> 50,000 NOK
Transaction frequency (30-day)	< 5 transactions	5-20 transactions	> 20 transactions
PEP status	Not PEP	PEP family member	PEP (direct)
Sanctions screening	Clear	Potential match (resolved)	Active match
Account age	> 12 months	3-12 months	< 3 months
Adverse media	None	Resolved/historical	Active negative coverage

Risk Level Classification

Total Score	Risk Level	Due Diligence	Monitoring	Transaction Limits
8-12	**Low**	Standard CDD (BankID only)	Quarterly re-screening	50,000 NOK/month
13-20	**Medium**	Enhanced CDD (BankID + document)	Monthly re-screening	25,000 NOK/month

Total Score	Risk Level	Due Diligence	Monitoring	Transaction Limits
21-30	**High**	Enhanced CDD + source of funds	Weekly re-screening	10,000 NOK/month
31+	**Prohibited**	Account blocked	Continuous	0 (blocked)

Database: `users` risk fields

Column	Type	Purpose
`risk_level`	TEXT	`low`, `medium`, `high`, `prohibited`
`pep_status`	TEXT	`none`, `pep_family`, `pep_direct`
`sanctions_cleared`	INTEGER	0 = not cleared, 1 = cleared

AML Transaction Monitoring

Alert Rules

Rule ID	Alert Type	Trigger	Severity	Description
AML-001	`structuring`	Multiple transactions just below 10,000 NOK threshold	`high`	Potential structuring to avoid reporting
AML-002	`velocity`	> 5 transactions in 1 hour	`medium`	Unusual transaction velocity
AML-003	`high_value`	Single transaction > 25,000 NOK	`medium`	Large transaction review
AML-004	`cumulative`	30-day total > 50,000 NOK	`high`	Cumulative volume threshold
AML-005	`corridor_risk`	Transfer to FATF grey/black list country	`high`	High-risk corridor
AML-006	`new_account_high_value`	Account < 30 days + transaction > 5,000 NOK	`medium`	New account with large transfer
AML-007	`round_amounts`	Multiple transactions with round amounts (1000, 5000, 10000)	`low`	Potential structuring pattern
AML-008	`rapid_recipient_add`	> 3 new recipients in 24 hours	`medium`	Unusual recipient creation pattern

Database: `aml_alerts` table

Column	Type	Values
`alert_type`	TEXT	`structuring`, `velocity`, `high_value`, `cumulative`, `corridor_risk`, etc.
`severity`	TEXT	`low`, `medium`, `high`, `critical`
`status`	TEXT	`open`, `investigating`, `resolved`, `escalated`, `filed`
`reviewed_by`	TEXT	Compliance officer identifier

Alert Lifecycle

```
stateDiagram-v2
    [*] --> open : Rule triggered
    open --> investigating : Compliance officer reviews
    investigating --> resolved : False positive confirmed
    investigating --> escalated : Suspicious activity confirmed
    escalated --> filed : STR filed with Okokrim
    resolved --> [*]
    filed --> [*]

    note right of escalated
        Auto-block user transactions
        until STR processed
    end note
```

SAR/STR Filing

When an AML alert is escalated, a Suspicious Transaction Report (STR) is filed with Okokrim/EFE (Norwegian Financial Intelligence Unit) per hvitvaskingsloven section 4-26.

STR Filing Trigger Conditions

Condition	Action	Timeline
AML alert severity = `critical`	Automatic STR draft + compliance notification	Immediately

Condition	Action	Timeline
AML alert escalated to `filed`	STR submitted to Okokrim	Within 24 hours of escalation
Compliance officer judgment	Manual STR creation	As determined
User account matches sanctions list	Immediate freeze + STR	Immediately

Database: `str_reports` table

Column	Type	Values
`report_type`	TEXT	`suspicious_transaction`, `sanctions_match`, `terrorism_financing`
`status`	TEXT	`draft`, `submitted`, `acknowledged`
`filed_at`	TEXT	Timestamp of submission to Okokrim
`reference_number`	TEXT	Okokrim reference (returned on submission)

STR Content (per hvitvaskingsloven section 4-26)

Field	Source	Description
Reporter details	Drop company info	ALAI Holding AS, org number, contact
Subject details	`users` table	Name, DOB, national_id_hash, address
Transaction details	`transactions` table	Amount, currency, date, recipient, corridor
Suspicious indicators	`aml_alerts` table	Alert type, pattern description, severity
Supporting evidence	`audit_log` table	Login history, transaction history, behavioral anomalies
Reporter assessment	Compliance officer	Narrative summary of suspicion basis

---

Ongoing Monitoring Schedule

Activity	Frequency	Scope	Automated

PEP/sanctions re-screening	Quarterly (low risk), Monthly (medium), Weekly (high)	All active users at applicable risk level	Yes (Sumsub batch API)
Transaction pattern analysis	Real-time	All transactions	Yes (AML rule engine)
Cumulative volume check	Daily	All users with transactions in last 30 days	Yes (scheduled job)
High-risk corridor review	Weekly	Users with transfers to FATF grey/black list countries	Yes (automated report)
Dormant account review	Monthly	Accounts with no activity for 6+ months then sudden activity	Yes (scheduled job)
Full compliance audit	Annually	All users, all transactions, all alerts	Manual + automated

---

GDPR Data Minimization for KYC Data

Per GDPR Article 5(1)(c) and Article 25 (data protection by design), KYC data collection and retention must be minimized.

Data Retention Table

Data Category	Data Elements	Retention Period	Legal Basis	Deletion Method
Identity (BankID)	national_id_hash, name, DOB	5 years after account closure	Hvitvaskingsloven s. 4-18 (AML record keeping)	Hard delete after retention
KYC documents	Passport/ID images, selfie	5 years after account closure	Hvitvaskingsloven s. 4-18	Sumsub retention + local reference deletion
Screening results	PEP/sanctions/media results	5 years after last screening	Hvitvaskingsloven s. 4-18	Hard delete after retention
AML alerts	Alert details, investigation notes	5 years after alert closure	Hvitvaskingsloven s. 4-18	Hard delete after retention
STR reports	Filed reports, evidence packages	10 years after filing	Hvitvaskingsloven s. 4-19 (STR records)	Hard delete after retention
Transaction records	Amount, currency, parties, timestamps	5 years after transaction	Bokforingsloven (accounting law)	Hard delete after retention
Consent records	Consent type, granted/withdrawn timestamps	Duration of relationship + 3 years	GDPR Art. 7(1) (proof of consent)	Hard delete after retention

Data Category	Data Elements	Retention Period	Legal Basis	Deletion Method
Audit logs	User actions, IP addresses, user agents	2 years	Legitimate interest (security)	Hard delete after retention

Data Minimization Controls

Control	Implementation	GDPR Article
Collect only necessary data	BankID provides verified name + DOB; no separate address collection until needed	Art. 5(1)(c)
Purpose limitation	KYC data used only for AML compliance, not marketing	Art. 5(1)(b)
Storage limitation	Automated retention policies with scheduled deletion jobs	Art. 5(1)(e)
Pseudonymization	National ID stored as SHA-256 hash, not plaintext	Art. 25
Access control	KYC data accessible only to compliance role	Art. 25
Right to erasure	Soft delete (set `deleted_at`) but retain AML-required data for legal period	Art. 17(3)(b)
Data portability	`GET /api/user/data-export` exports all personal data as JSON	Art. 20

Conflict: GDPR Erasure vs AML Retention

When a user requests account deletion (`DELETE /api/user/account`):

1. User record is soft-deleted (`deleted_at` timestamp set)
2. Active sessions are revoked
3. A `data_access_request` record is created (type: `erasure`, status: `completed`)
4. **AML-required data is RETAINED** for 5 years per hvitvaskingsloven s. 4-18
5. Response includes: `"retentionNote": "Data retained for 5 years per AML requirements"`

This is legally permitted under GDPR Article 17(3)(b): "compliance with a legal obligation which requires processing by Union or Member State law."

Cross-References

- Registration & Onboarding Flow -- User registration with KYC trigger

- System Context (C4 Level 1) -- Sumsub and Okokrim external actors
- Sumsub KYC Integration -- Technical integration specification
- Database Schema -- Compliance tables (aml_alerts, str_reports, screening_results, consents)
- Compliance Status -- Current compliance readiness
- ADR-003: PSD2 Pass-through -- Regulatory context
- Data Lifecycle -- Full data retention and deletion policies

---

Revision #4
Created 2026-02-21 05:58:52 UTC by John
Updated 2026-05-23 10:51:52 UTC by John