Data Lifecycle

Data Lifecycle Management

Version: 1.0 **Date:** 2026-02-21 **Status:** Approved **Owner:** Database Architect

---

Overview

Drop processes personal and financial data subject to multiple overlapping regulatory frameworks. This document defines retention periods, archival strategies, deletion cascades, and GDPR data subject request handling for all 19 tables.

Applicable regulations:

- **GDPR** (Personopplysningsloven, LOV-2018-06-15-38) -- data minimization, right to erasure, right to access
- **AML/KYC** (Hvitvaskingsloven, LOV-2018-06-01-23) -- 5-year retention post-relationship
- **Norwegian Bookkeeping Act** (Bokforingsloven) -- 5-year retention for financial records
- **PSD2** (Betalingstjenesteloven) -- audit trail requirements
- **Finansavtaleloven** -- complaint handling records

Key tension: GDPR right to erasure (Art. 17) vs. AML legal retention obligations. AML wins -- data required for anti-money laundering must be retained for 5 years regardless of erasure requests.

Retention Periods

Per-Table Retention Schedule

Table	Retention Period	Legal Basis	Archival After	Purge After
`users`	5 years post-relationship end	Hvitvaskingsloven section 30	Account deletion + 1 year	5 years post-deletion
`bank_accounts`	5 years post-relationship end	Hvitvaskingsloven section 30	Account deletion	5 years post-deletion

Table	Retention Period	Legal Basis	Archival After	Purge After
`transactions`	5 years from transaction date	Bokforingsloven section 13, Hvitvaskingsloven section 30	1 year after transaction	5 years after transaction
`recipients`	5 years post-relationship end	Hvitvaskingsloven section 30 (counterparty records)	Account deletion	5 years post-deletion
`merchants`	5 years post-relationship end	Bokforingsloven, Hvitvaskingsloven	Account deletion	5 years post-deletion
`sessions`	90 days after expiry	Legitimate interest (security)	After expiry	90 days after expiry
`notifications`	1 year from creation	Legitimate interest (UX)	6 months	1 year
`settings`	Duration of relationship	Contract performance	Account deletion	Immediate on deletion
`exchange_rates`	Indefinite (reference data)	Legitimate interest	Never	Never
`cards`	5 years post-cancellation	PCI-DSS, Bokforingsloven	Card cancellation	5 years post-cancellation
`spending_limits`	Duration of card lifecycle	Contract performance	Card cancellation	With card record
`rate_limits`	Until window expires	Legitimate interest (security)	Auto-cleaned per request	Immediate on expiry
`audit_log`	5 years from event	PSD2 Art. 94, Hvitvaskingsloven	1 year after event	5 years after event
`aml_alerts`	5 years post-resolution	Hvitvaskingsloven section 30	After resolution	5 years post-resolution
`str_reports`	5 years after filing	Hvitvaskingsloven section 30	Never (active reference)	5 years after filing
`screening_results`	5 years post-relationship end	Hvitvaskingsloven section 30	Account deletion	5 years post-deletion
`consents`	Duration of consent + 5 years	GDPR Art. 7(1) (proof of consent)	After withdrawal + 1 year	5 years after withdrawal
`data_access_requests`	5 years from completion	GDPR accountability (Art. 5(2))	After completion	5 years after completion
`complaints`	5 years from resolution	Finansavtaleloven, Bokforingsloven	After resolution	5 years after resolution

Per-Column Retention (Sensitive Fields)

Table.Column	Contains	Retention	Anonymization Method
`users.email`	PII (email address)	Until erasure (then anonymized)	Replace with `deleted_usr_{hash}@anonymized.local`
`users.first_name`	PII	Until erasure	Replace with `[REDACTED]`
`users.last_name`	PII	Until erasure	Replace with `[REDACTED]`
`users.phone`	PII	Until erasure	Replace with `NULL`
`users.date_of_birth`	PII	Until erasure	Replace with `NULL`
`users.national_id_hash`	PII (hashed)	5 years (AML)	Already hashed; set to `NULL` after retention
`users.password_hash`	Auth credential	Until erasure	Replace with `DELETED`
`bank_accounts.account_number`	Financial PII	5 years (AML)	Replace with `****{last4}`
`bank_accounts.iban`	Financial PII	5 years (AML)	Replace with `****{last4}`
`recipients.bank_account`	Financial PII	5 years (AML)	Replace with `****{last4}`
`recipients.name`	PII	5 years (AML, counterparty)	Replace with `[REDACTED]`
`cards.last_four`	Financial (partial)	5 years	Already truncated
`cards.pin_hash`	Auth credential	Until card cancellation	Set to `NULL`
`audit_log.ip_address`	PII (IP address)	5 years (PSD2)	Replace with `0.0.0.0` after retention
`audit_log.user_agent`	Quasi-PII	5 years	Replace with `[REDACTED]` after retention
`consents.ip_address`	PII	5 years (proof of consent)	Replace with `0.0.0.0` after retention

---

Archival Strategy

Active vs. Archived Data

```
flowchart LR
    A[Active Data<br/>Primary Database] -->|After retention trigger| B[Cold Archive<br/>Read-only Storage]
    B -->|After full retention period| C[Purge<br/>Permanent Deletion]

    subgraph "Active (PostgreSQL)"
        A1[Recent transactions]
```

```
        A2[Active users]
        A3[Current sessions]
    end

    subgraph "Cold Archive (S3/Glacier)"
        B1[Old transactions > 1 year]
        B2[Deleted user records]
        B3[Resolved AML alerts]
        B4[Filed STR reports]
    end

    subgraph "Purge"
        C1[Records past 5-year retention]
        C2[Anonymized analytics retained]
    end
```

Archival Tiers

Tier	Storage	Access Time	Data Types	Cost
Hot (Active DB)	PostgreSQL	Milliseconds	All current data, active users, recent transactions	Primary DB cost
Warm (Archive DB)	PostgreSQL read replica or separate schema	Seconds	Transactions > 1 year, deleted users pending retention	Reduced compute
Cold (Object storage)	AWS S3 / Glacier	Minutes to hours	Compliance exports, old audit logs, filed STR reports	Minimal

Archival Process

1. **Daily job:** Identify records eligible for archival (past active retention period)
2. **Export:** Write eligible records to archive storage (S3 with server-side encryption)
3. **Verify:** Confirm archive integrity (checksum comparison)
4. **Remove from active:** Delete from primary database
5. **Log:** Record archival action in `audit_log`

Deletion Cascades: User Account Deletion

When a user requests account deletion (GDPR Art. 17 right to erasure), the following cascade executes:

```
flowchart TD
    A[DELETE /api/user/account] --> B{Active transactions?}
    B -->|Yes, processing| C[Reject: Wait for completion]
    B -->|No| D[Begin deletion cascade]

    D --> E[Revoke all sessions]
    E --> F[Soft-delete user record]
    F --> G[Anonymize PII fields]
    G --> H[Create data_access_request<br/>type=erasure, status=completed]

    subgraph "Immediate Actions"
        E
        F
        G
    end

    subgraph "Retained for AML (5 years)"
        I[transactions — amounts, dates, types]
        J[audit_log — anonymized entries]
        K[aml_alerts — if any]
        L[str_reports — if any]
        M[screening_results — if any]
    end

    subgraph "Deleted Immediately"
        N[settings — preferences]
        O[notifications — all]
        P[rate_limits — if any for user IP]
    end

    subgraph "Anonymized + Retained"
        Q[bank_accounts — account numbers masked]
```

```
        R[recipients — names redacted]
        S[consents — IP anonymized]
    end

    H --> I
    H --> J
    H --> K
    H --> N
    H --> Q
```

Deletion Cascade Detail

Step	Table	Action	SQL
1	`sessions`	Revoke all	`UPDATE sessions SET revoked = 1 WHERE user_id = ?`
2	`users`	Soft delete + anonymize	`UPDATE users SET deleted_at = CURRENT_TIMESTAMP, email = 'deleted_' || id || '@anonymized.local', first_name = '[REDACTED]', last_name = '[REDACTED]', phone = NULL, date_of_birth = NULL, password_hash = 'DELETED' WHERE id = ?`
3	`settings`	Delete	`DELETE FROM settings WHERE user_id = ?`
4	`notifications`	Delete	`DELETE FROM notifications WHERE user_id = ?`
5	`bank_accounts`	Anonymize	`UPDATE bank_accounts SET account_number = '****' || RIGHT(account_number, 4), iban = CASE WHEN iban IS NOT NULL THEN '****' || RIGHT(iban, 4) END WHERE user_id = ?`
6	`recipients`	Anonymize	`UPDATE recipients SET name = '[REDACTED]', bank_account = '****' || RIGHT(bank_account, 4) WHERE user_id = ?`
7	`consents`	Anonymize IP	`UPDATE consents SET ip_address = '0.0.0.0' WHERE user_id = ?`
8	`cards`	Anonymize	`UPDATE cards SET pin_hash = NULL WHERE user_id = ?`
9	`spending_limits`	Delete	`DELETE FROM spending_limits WHERE user_id = ?`

Step	Table	Action	SQL
10	`data_access_requests`	Create record	`INSERT INTO data_access_requests (id, user_id, request_type, status, completed_at) VALUES (?, ?, 'erasure', 'completed', CURRENT_TIMESTAMP)`
11	`audit_log`	Log deletion	`INSERT INTO audit_log (id, user_id, action, details) VALUES (?, ?, 'user.deleted', '{"reason":"gdpr_erasure"}')`

NOT deleted (AML retention): `transactions`, `audit_log` (existing entries), `aml_alerts`, `str_reports`, `screening_results`, `merchants`. These are retained for 5 years per hvitvaskingsloven section 30, with PII fields anonymized.

Data Subject Access Request (DSAR) Implementation

DSAR Types

Request Type	GDPR Article	SLA	Implementation
Export (right to access)	Art. 15	30 days	`GET /api/user/data-export` -- returns JSON with all user data
Erasure (right to be forgotten)	Art. 17	30 days	`DELETE /api/user/account` -- soft delete + anonymization cascade
Rectification (right to correct)	Art. 16	30 days	`POST /v1/user/rectification` -- updates specified fields, creates data_access_request record
Restriction (right to restrict)	Art. 18	30 days	`POST /v1/user/restriction` -- flags account as restricted, creates data_access_request record

Export Flow

```
sequenceDiagram
    participant U as User
    participant API as API
    participant DB as Database

    U->>API: GET /api/user/data-export
    API->>DB: SELECT * FROM users WHERE id = ?
    API->>DB: SELECT * FROM transactions WHERE user_id = ?
    API->>DB: SELECT * FROM recipients WHERE user_id = ?
    API->>DB: SELECT * FROM bank_accounts WHERE user_id = ?
    API->>DB: SELECT * FROM settings WHERE user_id = ?
    API->>DB: SELECT * FROM consents WHERE user_id = ?

    API->>DB: INSERT INTO data_access_requests<br/>(type='export', status='completed')

    API-->>U: 200 JSON { user, transactions, recipients, bankAccounts, settings, consents }
```

The current implementation (`/api/user/data-export`) returns data inline as JSON. For production, large exports should be written to a temporary signed S3 URL and the `download_url` field in `data_access_requests` populated.

DSAR Tracking

All DSARs are tracked in the `data_access_requests` table:

Field	Purpose
`request_type`	export, erasure, rectification, restriction
`status`	pending -> processing -> completed/rejected
`requested_at`	When the user submitted the request
`completed_at`	When the request was fulfilled
`download_url`	Temporary URL for data export files
`notes`	Internal processing documentation

Anonymization Techniques

For Analytics Retention

After the active retention period, data can be anonymized for analytics rather than deleted:

Data Type	Anonymization Technique	Reversible?	Analytics Value
User identity	Replace name/email with opaque ID	No	User-level metrics without PII
Transaction amounts	Retain exact values (not PII)	N/A	Revenue and volume analytics
Geographic data	Retain country codes only	N/A	Corridor analysis
Timestamps	Retain date, remove time	Partially	Trend analysis
IP addresses	Replace with `0.0.0.0`	No	None (removed for privacy)
Bank account numbers	Replace with `****{last4}`	No	None
Phone numbers	Remove entirely	No	None

Anonymization SQL Pattern

```
-- Anonymize a deleted user's data for analytics retention
UPDATE users SET
    email = 'anon_' || id || '@analytics.internal',
    first_name = '[ANON]',
    last_name = '[ANON]',
    phone = NULL,
    date_of_birth = NULL,
    national_id_hash = NULL,
    password_hash = 'ANONYMIZED'
WHERE id = ? AND deleted_at IS NOT NULL;

-- Transaction data is retained as-is (amounts are not PII)
-- Recipient names are redacted
UPDATE recipients SET
    name = 'Recipient_' || id,
    bank_account = '****' || SUBSTR(bank_account, -4)
WHERE user_id = ?;
```

Legal Basis Reference

Retention Obligation	Law	Section	Requirement

KYC/AML records	Hvitvaskingsloven	Section 30	Retain customer identity and transaction records for 5 years after relationship ends
Transaction records	Bokforingsloven	Section 13	Retain accounting records for 5 years (3.5 years primary, 1.5 years secondary)
Audit trail	PSD2 / Betalingstjenesteloven	Art. 94 impl.	Maintain records of payment transactions for at least 5 years
Consent proof	GDPR	Art. 7(1)	Demonstrate that consent was given (retain proof)
Complaint records	Finansavtaleloven	Section 3-53	Maintain complaint records (15 business day response SLA)
Right to erasure exceptions	GDPR	Art. 17(3)(b)	Erasure does not apply when processing is necessary for compliance with legal obligation
Data minimization	GDPR	Art. 5(1)(c)	Do not retain data longer than necessary for stated purpose
STR records	Hvitvaskingsloven	Section 30	STR reports and supporting documentation retained 5 years after filing

Conflict resolution: When GDPR right to erasure conflicts with AML retention requirements, AML wins per GDPR Art. 17(3)(b). The user is informed that "data [is] retained for 5 years per AML requirements" in the deletion response.

Automated Lifecycle Jobs

Job	Frequency	Action
Session cleanup	Daily	Delete expired sessions older than 90 days
Rate limit cleanup	Every 100 rate limit checks	Delete expired rate limit entries (implemented in `middleware/rate-limit.ts`)
Notification cleanup	Weekly	Archive notifications older than 6 months, delete older than 1 year

Job	Frequency	Action
Audit log archival	Monthly	Move audit entries older than 1 year to cold storage
AML alert archival	Monthly	Archive resolved alerts older than 1 year
User data purge	Monthly	Permanently delete anonymized user data past 5-year retention
Consent proof archival	Monthly	Archive withdrawn consents older than 1 year

Retention Cron Endpoint

The retention enforcement is implemented as `GET /v1/cron/retention` (see `cron.ts`). When triggered, it:

1. **User anonymization** (5+ years post-deletion): Anonymizes PII fields (`email`, `first_name`, `last_name`, `phone`, `date_of_birth`, `national_id_hash`, `password_hash`) for users deleted more than 5 years ago
2. **Session cleanup**: Deletes expired sessions older than 90 days
3. **OTP cleanup**: Removes expired OTP codes (legacy table, wrapped in try/catch)

This endpoint should be called periodically (e.g., daily via external scheduler or cron job). It is not automatically scheduled within the application.

Cross-References

- **Database schema:** DATABASE-SCHEMA.md
- **Database design:** database-design.md
- **Audit architecture:** audit-architecture.md
- **Compliance status:** COMPLIANCE.md
- **Security architecture:** SECURITY-ARCHITECTURE.md
- **GDPR API endpoints:** API-REFERENCE.md (GDPR & Compliance section)
- **Account deletion:** `DELETE /api/user/account` in API-REFERENCE.md
- **Data export:** `GET /api/user/data-export` in API-REFERENCE.md

Revision #5
Created 2026-02-21 05:59:06 UTC by John
Updated 2026-05-23 10:57:17 UTC by John