Data Processing Agreements

- DPA Template
- DPA — Swan
- DPA — Sumsub
- DPA — Sentry

DPA Template

Data Processing Agreement (DPA)

Between:

- **Data Controller:** ALAI Holding AS, Org. No. 932 516 136 ("Controller")
- **Data Processor:** [PROCESSOR NAME], [Org. No.] ("Processor")

Effective Date: [DATE] **Product:** Drop payment services (getdrop.no)

---

1. Background and Purpose

1.1. This Data Processing Agreement ("DPA") is entered into pursuant to Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Norwegian Personal Data Act (LOV-2018-06-15-38).

1.2. The DPA governs the Processor's processing of personal data on behalf of the Controller in connection with the services described in Appendix 1.

1.3. This DPA is an integral part of the main service agreement between the parties dated [DATE] ("Main Agreement").

---

2. Definitions

Terms used in this DPA shall have the same meaning as defined in GDPR Article 4, unless otherwise specified.

---

3. Scope of Processing

3.1. The Processor shall only process personal data on behalf of the Controller and in accordance with the Controller's documented instructions (Appendix 1).

3.2. The scope, nature, purpose, and duration of processing, as well as categories of data subjects and types of personal data, are specified in Appendix 1.

3.3. The Processor shall not process personal data for its own purposes or for purposes beyond the scope of this DPA.

---

4. Controller's Obligations

4.1. The Controller is responsible for ensuring that there is a lawful basis for the processing of personal data under this DPA.

4.2. The Controller shall provide documented instructions for the processing of personal data. If the Processor believes that an instruction infringes GDPR or other data protection provisions, the Processor shall immediately inform the Controller.

---

5. Processor's Obligations

5.1. The Processor shall:

(a) Process personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required by EU or Member State law;

(b) Ensure that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Take all measures required pursuant to GDPR Article 32 (security of processing);

(d) Respect the conditions for engaging sub-processors as set out in Section 7;

(e) Assist the Controller in fulfilling its obligation to respond to data subject rights requests (GDPR Articles 15-22);

(f) Assist the Controller in ensuring compliance with GDPR Articles 32-36;

(g) At the choice of the Controller, delete or return all personal data after the end of the provision of services, and delete existing copies unless EU or Member State law requires storage;

(h) Make available to the Controller all information necessary to demonstrate compliance with Article 28, and allow for and contribute to audits.

6. Security Measures

6.1. The Processor shall implement appropriate technical and organizational security measures in accordance with GDPR Article 32, including:

(a) Pseudonymization and encryption of personal data; (b) Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems; (c) Ability to restore availability and access to personal data in a timely manner after an incident; (d) Regular testing and evaluation of the effectiveness of security measures.

6.2. Specific security measures are described in Appendix 2.

7. Sub-processors

7.1. The Controller provides general authorization for the Processor to engage sub-processors, subject to the conditions in this section.

7.2. The Processor shall maintain an up-to-date list of sub-processors available to the Controller upon request.

7.3. The Processor shall inform the Controller of intended changes concerning sub-processors at least 30 days in advance.

7.4. Sub-processors shall be bound by the same data protection obligations as set out in this DPA.

7.5. The Processor remains fully liable for sub-processor performance.

8. International Transfers

8.1. The Processor shall not transfer personal data outside the EEA without prior written consent.

8.2. Approved transfers shall be subject to appropriate safeguards (SCCs, adequacy decisions, or other GDPR Chapter V mechanisms).

9. Data Breach Notification

9.1. The Processor shall notify the Controller without undue delay (within 24 hours maximum) after becoming aware of a personal data breach.

9.2. The notification shall include: nature of breach, categories and number of records affected, likely consequences, and measures taken.

9.3. The Processor shall cooperate in investigating and resolving the breach.

---

10. Audit Rights

10.1. The Controller or its designated auditor may conduct audits of the Processor's compliance with this DPA.

10.2. Audits during normal business hours with minimum 14 days notice, unless triggered by a breach or regulatory investigation.

---

11. Duration and Termination

11.1. This DPA remains in effect for the duration of the Main Agreement.

11.2. Upon termination, the Processor shall delete or return all personal data within 30 days and certify deletion in writing.

---

12. Governing Law

12.1. This DPA is governed by Norwegian law.

Appendix 1 — Processing Details

Field	Description
Purpose	[Describe the specific service]
Nature	[Collection, storage, analysis, etc.]
Duration	Duration of Main Agreement
Data subjects	[End users, merchants, etc.]

Field	Description
Data types	[Name, email, transaction data, etc.]
Special categories	None (unless specified)

Appendix 2 — Security Measures

1. **Encryption:** [e.g., TLS 1.3 in transit, AES-256 at rest]
2. **Access Control:** [e.g., RBAC, MFA, least privilege]
3. **Logging:** [e.g., audit logging for all data access]
4. **Backup:** [e.g., daily encrypted backups]
5. **Incident Response:** [e.g., documented plan]
6. **Certifications:** [e.g., SOC 2 Type II, ISO 27001]

Signatures

Data Controller — ALAI Holding AS

Name: _____ Title: _____ Date: _____

Data Processor — [PROCESSOR NAME]

Name: _____ Title: _____ Date: _____

DPA — Swan

Data Processing Agreement — Swan

Between:

- **Data Controller:** ALAI Holding AS, Org. No. 932 516 136 ("Controller")
- **Data Processor:** Swan SAS ("Processor")

Effective Date: [DATE] **Product:** Drop payment services — Banking-as-a-Service (BaaS)

This DPA supplements the generic DPA template (`dpa-template.md`) with Swan-specific processing details. All general terms from the template apply unless overridden below.

Appendix 1 — Processing Details

Field	Description
Purpose	Banking infrastructure for Drop: account management, payment initiation (PISP), account information (AISP), transaction processing, and regulatory reporting via Swan's BaaS platform
Nature	Collection, storage, processing, and transmission of financial and identity data for payment services
Duration	Duration of BaaS service agreement between Controller and Swan
Data subjects	Drop end users (account holders), payment recipients, merchants accepting QR payments
Data types	Full name, IBAN/account number, bank name, transaction data (amount, currency, timestamp, reference), exchange rates, payment status, balance information, payment initiation requests, beneficiary details for remittance
Special categories	None

Appendix 2 — Security Measures (Swan)

1. **Encryption:** TLS 1.3 in transit; AES-256 at rest; HSM for cryptographic key management
2. **Access Control:** RBAC with MFA, segregation of duties, principle of least privilege
3. **Data Residency:** EU data centers (France) — all data processed within EEA
4. **Logging:** Complete audit trail for all financial transactions and API access
5. **Data Retention:** Transaction data retained per Controller instructions (aligned with bokfoeringsloven 5-year requirement); account data retained during relationship + regulatory period
6. **Incident Response:** 24/7 security operations, breach notification within 24 hours
7. **Certifications:** PCI DSS Level 1, licensed by ACPR (French banking regulator), PSD2 compliant
8. **Financial Regulations:** Compliant with PSD2, EMD2, and applicable French/EU banking regulations

---

Additional Swan-Specific Terms

Regulatory Compliance

- Swan operates as a licensed payment institution under French law, supervised by ACPR
- Processing of payment data complies with PSD2 requirements for strong customer authentication (SCA)
- Transaction data available for regulatory reporting to Norwegian authorities (Finanstilsynet) upon Controller's request

Payment Data

- All payment initiation and account information services comply with PSD2 PISP/AISP requirements
- Transaction data includes full audit trail with timestamps, amounts, currencies, and counterparty information
- Idempotency controls prevent duplicate transactions

Data Subject Rights

- Swan shall assist Controller in responding to data subject requests within 10 business days

- Account data and transaction history exportable in machine-readable format (JSON/CSV)
- Data erasure subject to regulatory retention requirements (minimum 5 years for financial records)

Business Continuity

- Redundant infrastructure with 99.9% uptime SLA
- Regular disaster recovery testing
- Data backup with point-in-time recovery capability

Signatures

Data Controller — ALAI Holding AS

Name: _____ Title: _____ Date: _____

Data Processor — Swan SAS

Name: _____ Title: _____ Date: _____

DPA — Sumsub

Data Processing Agreement — Sumsub

Between:

- **Data Controller:** ALAI Holding AS, Org. No. 932 516 136 ("Controller")
- **Data Processor:** Sumsub Limited ("Processor")

Effective Date: [DATE] **Product:** Drop payment services — KYC/Identity Verification

---

This DPA supplements the generic DPA template (`dpa-template.md`) with Sumsub-specific processing details. All general terms from the template apply unless overridden below.

Appendix 1 — Processing Details

Field	Description
Purpose	Identity verification (KYC/CDD) for Drop users, including document verification, liveness checks, PEP screening, and sanctions list checks in accordance with Norwegian AML legislation (hvitvaskingsloven)
Nature	Collection, verification, storage, and analysis of identity documents and biometric data
Duration	Duration of service agreement between Controller and Sumsub
Data subjects	Drop end users (natural persons in Norway applying for or holding Drop accounts)
Data types	Full name, date of birth, national ID number (encrypted), nationality, identity document images (passport/ID card), selfie/liveness capture, PEP screening results, sanctions check results, risk score, verification status
Special categories	Biometric data for identity verification (GDPR Art. 9(2)(g) — substantial public interest: AML obligations)

Appendix 2 — Security Measures (Sumsub)

1. **Encryption:** TLS 1.3 in transit; AES-256 at rest for all stored documents and data
2. **Access Control:** Role-based access, MFA for all staff, principle of least privilege
3. **Data Residency:** EU data centers (primary processing within EEA)
4. **Logging:** Comprehensive audit trail for all verification events and data access
5. **Data Retention:** Verification data retained for the period specified by Controller (aligned with hvitvaskingsloven 5-year requirement), then securely deleted
6. **Incident Response:** 24/7 security operations, breach notification within 24 hours
7. **Certifications:** SOC 2 Type II, ISO 27001, PCI DSS compliant
8. **Sub-processors:** List maintained and available at Sumsub's sub-processor page; 30-day advance notice of changes

---

Additional Sumsub-Specific Terms

Biometric Data

- Biometric data (liveness/selfie) processed solely for identity verification purposes
- Not used for surveillance, profiling, or any purpose beyond KYC verification
- Deleted upon completion of verification cycle (not retained beyond verification outcome)

Data Subject Rights

- Sumsub shall assist Controller in responding to data subject access, erasure, and portability requests within 10 business days
- Verification results and risk scores can be exported in machine-readable format

Transfer Impact Assessment

- Primary processing: EU/EEA data centers
- Any processing outside EEA covered by EU SCCs (Decision 2021/914)
- TIA documentation available upon request

Signatures

Data Controller — ALAI Holding AS

Name: _____ Title: _____ Date: _____

Data Processor — Sumsub Limited

Name: _____ Title: _____ Date: _____

DPA — Sentry

Data Processing Agreement — Sentry

Between:

- **Data Controller:** ALAI Holding AS, Org. No. 932 516 136 ("Controller")
- **Data Processor:** Functional Software, Inc. dba Sentry ("Processor")

Effective Date: [DATE] **Product:** Drop payment services — Error Monitoring and Performance

---

This DPA supplements the generic DPA template (`dpa-template.md`) with Sentry-specific processing details. All general terms from the template apply unless overridden below.

Appendix 1 — Processing Details

Field	Description
Purpose	Application error monitoring, crash reporting, and performance tracking for the Drop application to ensure service reliability and rapid incident response
Nature	Collection, storage, and analysis of error reports, stack traces, and performance metrics
Duration	Duration of Sentry subscription agreement
Data subjects	Drop end users (indirectly, via error context), Drop application developers and administrators
Data types	Error messages and stack traces, request URLs and HTTP headers (redacted), IP addresses (anonymizable), browser/device information, user agent strings, request IDs, breadcrumb events, performance traces (transaction timing)
Special categories	None — financial data and PII are scrubbed before transmission to Sentry (see Data Scrubbing section)

Appendix 2 — Security Measures (Sentry)

1. **Encryption:** TLS 1.3 in transit; AES-256 at rest
2. **Access Control:** SSO/SAML, RBAC, MFA enforcement, IP allowlisting available
3. **Data Residency:** EU data region available (selected for Drop); data stored in EU
4. **Logging:** Access audit logs available via Sentry dashboard
5. **Data Retention:** Configurable retention (Controller sets to 90 days for error data); automatically purged after retention period
6. **Incident Response:** Sentry security incident response per SOC 2 procedures
7. **Certifications:** SOC 2 Type II
8. **Privacy:** Sentry does not sell or share customer data; processes data solely per Controller instructions

---

Additional Sentry-Specific Terms

Data Scrubbing (Controller Responsibility)

The Controller implements the following data scrubbing measures BEFORE data is transmitted to Sentry:

- **PII Filtering:** All user names, email addresses, phone numbers, and national ID numbers are stripped from error payloads using Sentry SDK's `beforeSend` hook
- **Financial Data:** Transaction amounts, account numbers, IBANs, and card numbers are never included in error reports
- **IP Anonymization:** IP addresses are anonymized (last octet zeroed) via Sentry SDK configuration
- **Request Body Filtering:** POST bodies containing financial or personal data are excluded from error reports
- **Custom Scrubbing Rules:** Sentry's server-side data scrubbing enabled for additional patterns (credit card, SSN)

Data Minimization

- Only error context necessary for debugging is transmitted
- User ID may be included for error correlation (pseudonymized identifier only)
- Request ID (correlation ID) included for log cross-referencing
- No financial transaction details, KYC data, or AML data transmitted to Sentry

Data Subject Rights

- Since data transmitted to Sentry is scrubbed of direct identifiers, data subject requests are primarily handled by the Controller
- If pseudonymized user IDs need to be purged, Controller can use Sentry's data deletion API
- Sentry supports GDPR data deletion requests via their API

Spike Protection

- Sentry spike protection prevents excessive data collection during error storms
- Controller configures rate limits to prevent inadvertent data over-collection

---

Signatures

Data Controller — ALAI Holding AS

Name: _____ Title: _____ Date: _____

Data Processor — Functional Software, Inc. dba Sentry

Name: _____ Title: _____ Date: _____