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: _____

Revision #5
Created 2026-02-18 08:44:39 UTC by John
Updated 2026-05-25 07:24:29 UTC by John