

Data Processing Terms

Stratum Intelligence Inc. · Version 1.2 · Effective June 2026

1. Scope and roles

These Data Processing Terms ("DPT") form part of the Stratum Master Services Agreement and govern Stratum's processing of Customer Personal Data on Customer's behalf. Customer is the Controller and Stratum is the Processor.

Where Customer acts as a Processor for its own end customers, Stratum acts as a Sub-processor and the same obligations flow down.

2. Subject matter and duration

Subject matter: provisioning and operating the Stratum operational intelligence platform.

Duration: for the term of the Agreement plus any period necessary for return or deletion of data.

3. Categories of data and data subjects

Categories of Personal Data: account identifiers, contact details of authorized users, audit metadata (IP, user-agent, timestamps), and any Personal Data embedded in telemetry the Customer chooses to send.

Categories of data subjects: Customer's employees, contractors, and end users.

4. Stratum obligations

Process Personal Data only on documented Customer instructions.

Ensure persons authorised to process Personal Data are bound by confidentiality.

Implement the technical and organisational measures in Annex A of this DPT.

Assist Customer with data subject requests, DPIAs, and regulator engagement.

Notify Customer of a Personal Data Breach without undue delay and no later than 48 hours after becoming aware.

5. Sub-processors

Customer authorises Stratum to engage the Sub-processors listed at </legal/subprocessors>. Stratum will provide at least 30 days' notice of additions, during which Customer may object on reasonable grounds.

6. International transfers

Transfers outside the EEA, UK, and Switzerland are made under the EU Standard Contractual Clauses (2021/914) and the UK Addendum, as applicable. Transfer Impact Assessments are available on request.

7. Return and deletion

On termination Stratum will delete or return Personal Data within 30 days, subject to legal retention obligations. Backups are purged on a rolling 35-day cycle.

8. Audits

Stratum will make available evidence of compliance, including the most recent SOC 2 Type II report under NDA, and will allow audits by Customer or its mandated auditor with reasonable prior notice no more than once per 12 months.

Annex A — Technical and organisational measures

- TLS 1.3 in transit and AES-256 at rest with managed KMS.
- Row-level security on every tenant table; least-privilege column grants on secrets.
- Role-based access control with owner/admin/operator/viewer separation.
- Outbound-only connector agents with mTLS device identity.
- Immutable audit log with tenant-scoped retention.
- Continuous vulnerability scanning and quarterly penetration testing.
- Annual security training and background checks for all personnel.