ComplianceSuite

FIT-CLEAN

CS-LEG-0001 · COMPLIANCESUITE DOCUMENTATION

Data Processing Agreement.

FIT-only redaction. Effective 2026-04-28.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-LEG-0001	v1.0	2026-04-28	Legal & Compliance

Public — Documentation · Review cycle: On change

01 — DOCUMENT CONTROL

Control block and metadata anchor.

The control block identifies the document, its current revision, the regulated process it supports, and the people accountable for its lifecycle. Every value below is the source of truth for any downstream record, audit trail entry, or signature block.

DOCUMENT ID	CS-LEG-0001
TITLE	Data Processing Agreement (Template)
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Legal & Compliance
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

02 — APPROVALS

Sign-off table, ready for ink or e-signature.

The signatures below confirm review and authorisation of this document. Approvals must be recorded in chronological order. If the document is signed electronically, the e-signature record on the ComplianceSuite platform supersedes any handwritten entry on this page and carries the same legal weight under 21 CFR Part 11 and EU GMP Annex 11.

Role	Name	Function	Date	Signature
Author		Validation Lead		
Reviewer		Quality Assurance		
Reviewer		Process / System Owner		
Approver		Head of Quality		
Approver		Regulatory Affairs		

03 — CONTENTS

What's in this document.

01 — WHAT THIS EDITION COVERS

What this edition covers.

- GDPR Art. 28 compliance — Processor obligations, Sub-Processor regime, Breach notification
- Standard Clauses — Processor instructions, Confidentiality, DSR support
- Technical and Organizational Measures (TOMs) — Encryption, Access control, Audit trail
- Audit rights — Documentation, SOC 2 Type II, ISO 27001 as first-line evidence
- International Transfers — Standard Contractual Clauses
- Return or deletion at end of lifecycle

04 — Disclaimer.

Note: This document is a template for legal professionals. It is not legal advice. The customer's legal team must review every clause against the customer's applicable law and regulation before signature. Placeholders are marked with <…>.

05 — Parties and Structure.

This Data Processing Agreement is entered into between:

- **Controller:** `<Customer legal entity>`
- **Processor:** `<ComplianceSuite legal entity>`

The DPA is part of the Master Services Agreement (MSA) between the parties.

Structure

06 — Processing Subject Matter and Duration.

2 — Processing Subject Matter and Duration

Element	Specification
Processing subject matter	Provision of the ComplianceSuite platform: creation of regulated datasets, approval processes, audit trail, inspection-ready export
Duration	For the term of the MSA plus the retention period specified in the MSA following termination
Nature	Storage, hosting, transmission, transformation (rendering), deletion
Purpose	Performance of Processor obligations under the MSA; no other use

3 — Categories of Personal Data and Data Subjects

Data subjects:

- Employees and authorized users of the customer
- Data subjects whose data the customer stores in its regulated datasets

Categories of personal data:

- Identity information (name, email, employee number)
- Authentication factors
- Audit trail metadata (IP address, user agent)
- Content that the customer includes in datasets

Special categories: The platform is not designed for processing of Art. 9 GDPR data unless expressly agreed in the MSA.

07 — Processor Obligations.

The Processor undertakes:

01 To process personal data only in accordance with documented instructions from the Controller, including international transfers; in case of legal obligation, to notify the Controller in advance.

01 To ensure that persons authorized to process personal data are under a confidentiality obligation.

01 To implement all measures required by Art. 32 GDPR.

01 To assist the Controller through technical and organizational measures in fulfilling data subject requests (Art. 12–22 GDPR).

01 To make available all information necessary to verify compliance.

08 — Sub-Processor Regime.

01 The Controller grants the Processor general written authorization to engage Sub-Processors.

01 The Processor maintains a current Sub-Processor list at `<URL — published endpoint>` (also reproduced in Annex C of this DPA).

01 The Processor notifies the Controller of changes (addition or replacement) with appropriate advance notice and gives the Controller an opportunity to object on reasonable grounds.

01 The Processor commits each Sub-Processor by contract to data protection obligations no less protective than those of this DPA.

01 The Processor is fully liable for the performance of its Sub-Processors.

09 — Security and Breach Notification.

7 — Security and Confidentiality

The Processor implements and maintains the Technical and Organizational Measures (TOMs) described in Annex B. The TOMs take account of the state of the art, costs of implementation, nature, scope, context and purpose of the processing, and risks to data subject rights.

8 — Breach Notification

01 The Processor notifies the Controller without undue delay upon becoming aware of a personal data breach.

01 The notification shall contain — where available: - Nature of the breach - Categories and approximate number of data subjects - Likely consequences - Measures taken or envisaged to mitigate

01 If information is not available in the initial notification, it shall be provided in phases.

10 — International Transfers.

For transfers from the EEA, UK or Switzerland to third countries without an adequacy decision:

01 The parties shall execute the EU Standard Contractual Clauses (2021/914) or applicable UK / Swiss equivalents.

01 The parties shall conduct a Transfer Impact Assessment pursuant to EDPB Recommendation 01/2020.

01 The customer tenant shall select a residency consistent with its regulatory obligations.

11 — Audit Rights.

01 The Processor shall make available all information necessary to demonstrate compliance and tolerate audits and inspections by the Controller or its authorized representative.

01 As first-line evidence serve the SOC 2 Type II Report and the ISO 27001 Alignment Statement (accessible under standard NDA).

01 If first-line evidence is insufficient, the Controller may request further information; the Processor shall respond within reasonable time.

01 On-site audits are reserved for cases not resolved through documentation. The parties shall agree on scope, timing and confidentiality in advance.

12 — Return or Deletion.

01 Upon termination or expiry of the MSA, the Processor shall make the data available in structured, machine-readable format at the Controller's election or delete it.

01 The Processor may retain data to the extent that Union or national law requires; in such case, the Processor shall identify the data and the legal basis.

01 Data retained for compliance continuity (audit trail following termination) shall be subject to the same security and confidentiality obligations as during the term of the MSA.

Annex A — Processing Description.

<Specification with party-specific values: data subjects, categories, duration, nature, purpose>

Annex B — Technical and Organizational Measures (TOMs).

Cryptography and Pseudonymization

- **In Transit:** TLS 1.3 (enforced via reverse-proxy configuration, Let's Encrypt certificates)
- **At Rest:** AES-256-GCM (standard in production database settings)
- **Pseudonymization:** Audit trail entries carry sequence number and hash reference, not session secrets

Confidentiality, Integrity, Availability, Resilience

- Multi-zone replication in primary cloud region
- Tested disaster recovery scenario
- Tamper-evident audit trail with sequence numbers
- RTO / RPO documented in Security Whitepaper

Availability Recovery

- Documented RTO / RPO per tier
- Backup retention per Service Order

Regular Effectiveness Review

- Annual penetration test
- Quarterly security position review
- ISO 27001 / SOC 2 Type II audit cycle per certification body

Access Control

- JWT authentication with RS256 signing
- Role-Based Access Control (RBAC) per tenant and system
- Argon2 password hashing

- Audit trail of every access (user, IP, user agent, action, timestamp)

Personnel Training

- Confidentiality obligations in employment contracts
- Annual security awareness training
- Background checks for personnel with access to customer data (where applicable by law)

Annex C — Approved Sub-Processor List.

<Current Sub-Processors with name, role, processing location. Maintained at published URL with real-time updates; current version at signature time reproduced here.>

13 — Liability and Governing Law.

Liability: Liability governed by MSA Clause 13.

Order of Precedence: In case of conflict: (1) Service Order, (2) DPA, (3) MSA, (4) other.

REVISION HISTORY

Every change, tracked and signed.

Add one row for every controlled revision. Minor changes (typos, formatting) increment the patch version; substantive edits trigger a fresh review cycle and a new approver round.

Version	Date	Author	Summary of Change	Approver
1.0	2026-04-28	Documentation Team	FIT-only redaction limited to codebase-verified functionality.	Head of Documentation
—	—	—	Reserved for next revision. Do not delete this row.	—

GLOSSARY

Shared language, no ambiguity.

Definitions used throughout this document. Where a term has a specific meaning inside ComplianceSuite, the platform-specific definition takes precedence over the generic regulatory term.

CSV	Computerized Systems Validation
GAMP 5	Good Automated Manufacturing Practice, Edition 5 (2nd edition, 2022)
GxP	Good 'x' Practice — covers GMP, GLP, GCP, GDP, GVP
IQ / OQ / PQ	Installation / Operational / Performance Qualification
Part 11	21 CFR Part 11 — US FDA rule on electronic records and electronic signatures
Annex 11	EU GMP Annex 11 — EU rule on computerised systems
URS	User Requirements Specification
FRS	Functional Requirements Specification
RTM	Requirements Traceability Matrix
SOP	Standard Operating Procedure
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
ICH Q9	International Council for Harmonisation Quality Risk Management guideline

— End of document —