GxP-Desk

FIT-CLEAN

CS-LEG-0001 · GXP-DESK DOCUMENTATION

Data Processing Agreement.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-LEG-0001	v1.0	2026-06-04	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	2026-06-04
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 GxP-Desk 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 VERSION COVERS

What this version covers.

- GDPR Art. 28 conformity — 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 jurisdiction and regulatory framework before it is signed. Placeholders are marked with <…>.

05 — Parties and Structure.

This Data Processing Agreement is entered into between:

- **Controller:** `<Customer legal entity>`
- **Processor:** `<GxP-Desk legal entity>`

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

Structure

06 — Subject Matter and Duration of Processing.

2 — Subject Matter and Duration of Processing

Element	Specification
Subject matter of processing	Provision of the GxP-Desk platform: creation of regulated records, approval workflows, audit trail, inspection-ready export
Duration	For the term of the MSA + the post-termination retention period specified in the MSA
Nature	Storage, hosting, transmission, transformation (rendering), deletion
Purpose	Performance of the 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 records

Categories of personal data:

- Identity information (name, email, employee number)
- Authentication factors
- Audit trail metadata (IP address, user agent)
- Content that the customer enters into records

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

07 — Processor Obligations.

The processor undertakes to:

01 Process personal data only in accordance with the controller's documented instructions, including in relation to international transfers; where required to do so by law, notify the controller in advance.

01 Ensure that persons authorized to process the data are bound by an obligation of confidentiality.

01 Take all measures required under Art. 32 GDPR.

01 Assist the controller, through technical and organizational measures, in fulfilling data subject requests (Art. 12–22 GDPR).

01 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 (additions or replacements) with reasonable advance notice and gives the controller the opportunity to object on reasonable grounds.

01 The processor binds each sub-processor by contract to data protection obligations no less protective than those of this DPA.

01 The processor remains 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 into account the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the risks to data subjects' rights.

8 — Breach Notification

01 The processor notifies the controller without undue delay after becoming aware of a personal data breach.

01 The notification includes — to the extent available: - The nature of the breach - The categories and approximate number of data subjects affected - The likely consequences - The measures taken or proposed to mitigate the breach

01 Where information is not available at the time of initial notification, it is provided in phases thereafter.

08 — 10 — INTERNATIONAL TRANSFERS

10 — International Transfers.

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

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

01 The parties carry out a transfer impact assessment in accordance with EDPB Recommendation 01/2020.

01 The customer tenant selects a data residency consistent with its regulatory obligations.

11 — Audit Rights.

01 The processor makes available all information necessary to demonstrate compliance and allows for and contributes to audits and inspections conducted by the controller or its mandated representative.

01 The SOC 2 Type II report and the ISO 27001 alignment statement (accessible under a standard NDA) serve as first-line evidence.

01 Where the first-line evidence is insufficient, the controller may request further information; the processor responds within a reasonable period.

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

12 — Return or Deletion.

01 Upon termination or expiry of the MSA, the processor, at the controller's choice, makes the data available in a structured, machine-readable format or deletes it.

01 The processor may retain data to the extent required by Union or national law; in that case, the processor identifies the data and the legal basis.

01 Data retained for compliance continuity (post-termination audit trail) remains subject to the same security and confidentiality obligations as during the MSA term.

Annex A — Description of Processing.

<To be completed 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); optional **BYOK** (customer CMK via AWS/Azure/GCP KMS, envelope encryption, key rotation)
- **Pseudonymization:** Audit trail entries carry a sequenceNumber and hash reference, not session secrets

Confidentiality, Integrity, Availability, Resilience

- Multi-zone replication; multi-region data residency EU/US selectable (`Tenant.dataRegion`)
- Tested disaster recovery scenario
- Tamper-evident audit trail with sequence numbers
- RTO / RPO documented in the security whitepaper

Availability Recovery

- Documented RTO / RPO per tier
- Backup retention per service order

Regular Review of Effectiveness

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

Access Control

- JWT authentication; **SSO via SAML 2.0 / OpenID Connect** with enforcement and domain routing
- **MFA** (WebAuthn/passkeys, TOTP, recovery codes); re-authentication on electronic signature
- 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 (in accordance with applicable law)

Annex C — List of Approved Sub-Processors.

<Current sub-processors with name, role, place of processing. Maintained at a published URL with real-time updates; the version current as of the time of signature is reproduced here.>

13 — Liability and Order of Precedence.

Liability: Liability is governed by MSA Clause 13.

Order of Precedence: In the event of conflict: (1) Service Order, (2) DPA, (3) MSA, (4) others.

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	2026-06-04	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 GxP-Desk, 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 —