Data Processing Agreement — Confinity v1 (template)

Version 1.0.0 · 2026Q2 · Last updated Thu Apr 23 2026 00:00:00 GMT+0000 (Coordinated Universal Time)

Data-Processing Agreement: Confinity v1 (template)

This is the contractual template Confinity signs with business customers. It is published here so any customer can read it before subscribing, download the PDF, or send a countersigned copy. The PDF under public/legal/confinity-dpa-v1.pdf is the canonical signable artefact; counsel will refresh that PDF when this MDX is cleared.

1. Definitions and interpretation

"Customer", "Controller", "Processor", "Sub-processor", "Personal Data", "Processing", "Data Subject", "EEA", and "Restricted Transfer" each have the meaning given in the UK GDPR and the EU GDPR respectively.

2. Processing of Customer Personal Data

Confinity processes Customer Personal Data only on Customer's documented instructions, as set out in this DPA and in the published product documentation. Processing purposes, data categories, and data-subject categories are described in Annex I.

3. Confinity's responsibilities

Confinity will:

- ensure persons authorised to process Customer Personal Data are under a duty of confidentiality;
- implement appropriate technical and organisational measures as set out in Annex II;
- assist Customer, insofar as possible, in fulfilling obligations relating to data-subject rights, DPIAs, prior consultation, and breach notification;
- make available information necessary to demonstrate compliance and allow for audits as described in Section 7;
- delete or return Customer Personal Data on termination as described in Section 10.

4. Sub-processors

Customer authorises Confinity to engage sub-processors listed on the public register at https://www.confinity.com/trust/centre/subprocessors. Confinity will notify Customer by email at least thirty (30) days before adding a new sub-processor that handles Customer Personal Data. Customer may object to the addition within twenty (20) days of notice; Confinity will work in good faith to address the objection, failing which Customer may terminate the affected Service without penalty.

5. International transfers

Where processing of Customer Personal Data involves a Restricted Transfer, the parties incorporate by reference the European Commission's Standard Contractual Clauses (2021/914, Module Two: Controller to Processor) and, for transfers out of the United Kingdom, the UK International Data Transfer Addendum as published by the ICO, each populated with the parties' details in Annex I.

6. Security measures (Annex II)

Confinity implements the technical and organisational measures set out in Annex II. Changes that materially weaken those measures require notice to Customer.

7. Audit rights and certifications

Confinity makes available to Customer, on written request, the most recent external attestations or certifications then in force (for example, SOC 2, ISO 27001, or equivalent). Customer may, no more than once per twelve-month period, request an audit; the parties will agree scope, timing, and cost in good faith.

8. Data-subject rights assistance

Confinity will, taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests for exercising data-subject rights under applicable Data Protection Laws.

9. Personal-data breach notification

Confinity will notify Customer without undue delay and in any event within forty-eight (48) hours after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notification is aligned with the Confinity unified SEV disclosure clock published at documentation/legal/sev-disclosure-clock.md.

10. Deletion or return of Customer Personal Data on termination

Upon termination of the Service, Confinity will, at Customer's choice, delete or return all Customer Personal Data and delete existing copies except to the extent applicable law requires storage. Industry-standard retention windows for billing and tax records are set out in Annex I.

11. Liability and indemnity

Each party's liability under this DPA is subject to the liability caps and exclusions in the underlying Confinity Services Agreement.

12. Jurisdiction and governing law

This DPA is governed by the governing law of the underlying Confinity Services Agreement. Disputes are resolved per that Agreement.

Annex I: Details of processing

- Subject matter of processing: delivery of the Confinity service.
- Duration of processing: term of the underlying Services Agreement

plus retention windows set out in the privacy policy.

- Nature and purpose: as described in the product documentation and

in the ROPA.

- Categories of personal data: as described in the ROPA.
- Categories of data subjects: account holders, contributors, family

members invited to a space, and third-party payment counterparties.

Annex II: Technical and organisational measures

- Encryption in transit (TLS).
- Encryption at rest: to be completed before execution. Confinity does

not presently apply application-layer encryption to entry content. The field-encryption path exists and is deliberately disabled, because it is not wired end to end. Whatever the hosting platform applies underneath has to be confirmed and stated here before this Annex is signed, and it is left open rather than filled in with an assumed value.

- Access controls with least-privilege defaults and auditable role

assignments.

- Backups as configured at the hosting platform. Restore-drill cadence to

be completed before execution: drill tooling exists in the repository, a recurring schedule does not.

- Logging with PII redaction at source (see Sentry wrapper + OTel

attribute allowlist).

• Independent external penetration test: first engagement not yet completed. Cadence to be stated before execution.

• Incident response playbook with the unified SEV disclosure clock.

Annex III: List of sub-processors

The current list is published at https://www.confinity.com/trust/centre/subprocessors and is incorporated by reference into this DPA. Updates trigger the notice process in Section 4.

Change log

• 2026-04-23: v1.0.0 initial template published.

Signature page

By signing below, Customer and Confinity agree to the Data Processing Agreement printed above as the binding contract for processing Customer Personal Data under the Confinity Services Agreement.

Confinity Ltd.

Signature: _____

Printed name: _____

Title: _____

Date: _____

Customer

Signature: _____

Printed name: _____

Title: _____

Date: _____