

Data Processing Addendum

EFFECTIVE DATE	LAST UPDATED
July 23, 2026	July 23, 2026

This Data Processing Addendum (“**DPA**”) forms part of the Master SaaS Subscription Agreement between Customer and Capital Connect Solutions, Corp. d/b/a CapConnect.

1 1. Scope and Roles

This DPA applies where CapConnect processes Personal Data on behalf of Customer in providing the Services.

Customer is the controller, business, or equivalent entity that determines the purposes and means of processing. CapConnect is the processor, service provider, contractor, or equivalent entity, except where CapConnect independently determines purposes and means for account administration, security, billing, fraud prevention, legal compliance, or its own permitted analytics.

2 2. Processing Instructions

CapConnect will process Personal Data only:

- to provide the Services and perform documented Customer instructions;
- as described in the Agreement and this DPA;
- to prevent or address security, fraud, abuse, or technical issues;
- as required by applicable law; or
- with Customer’s written authorization.

If CapConnect believes an instruction violates applicable data-protection law, it may notify Customer and suspend the affected processing until the parties resolve the issue.

3 3. Details of Processing

Subject matter: Hosting and operation of a revenue operations, sales orchestration, communications, analytics, and workflow platform.

Duration: The Subscription Term plus authorized retention and deletion periods.

Nature and purpose: Hosting, organizing, transmitting, enriching, analyzing, reporting, automating, securing, supporting, and deleting Customer Data.

Categories of data subjects: Customer personnel, leads, prospects, customers, vendors, business contacts, website visitors, and other individuals whose data Customer submits.

Types of Personal Data: Contact information, employment and company information, communication content and metadata, recordings and transcripts, engagement events, CRM and pipeline information, device and usage information, and other data chosen by Customer.

Sensitive data: Customer must not submit sensitive or regulated data unless the applicable Service and Order Form expressly permit it.

4 4. Confidentiality

CapConnect will ensure personnel authorized to process Personal Data are bound by confidentiality obligations and receive appropriate privacy and security guidance.

5 5. Security

CapConnect will implement reasonable technical and organizational measures described in the Security Addendum, taking into account the nature, scope, context, and purposes of processing and the risk to individuals.

6 6. Subprocessors

Customer authorizes CapConnect to use subprocessors. CapConnect will maintain a current subprocessor list or notice and impose written data-protection obligations materially consistent with this DPA.

CapConnect may add or replace subprocessors. Where legally required, CapConnect will provide notice and a reasonable opportunity to object based on documented data-protection concerns. If the parties cannot resolve a valid objection, Customer may terminate the affected Service as its exclusive remedy.

7 7. Individual Rights

Taking into account the nature of processing, CapConnect will provide commercially reasonable assistance enabling Customer to respond to verified requests for access, correction, deletion, portability, restriction, objection, or other applicable rights. CapConnect may charge reasonable fees for assistance beyond standard product functionality.

8 8. Security Incidents

CapConnect will notify Customer without undue delay after confirming a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed on Customer's behalf ("**Personal Data Breach**").

Notice will include available information reasonably needed for Customer's legal obligations. CapConnect's notice is not an admission of fault or liability. Customer is responsible for notifications to individuals and regulators unless law assigns that duty to CapConnect.

9 9. Data Protection Impact Assessments

CapConnect will provide reasonably available information to assist Customer with data-protection impact assessments and regulator consultations, taking into account the nature of processing. Additional assistance may be subject to fees.

10 10. Return and Deletion

Upon expiration or termination, CapConnect will delete or return Personal Data in accordance with the Agreement, unless law requires retention. Backup copies may remain until overwritten under standard retention cycles and will remain protected.

CapConnect may retain Aggregated Data, Derived Data, Platform Data, Usage Data, and De-identified Data that does not reasonably identify Customer or an individual.

11 11. Audits and Information

CapConnect will make available information reasonably necessary to demonstrate compliance with this DPA, including relevant third-party reports or summaries where available.

No more than once annually, Customer may request a remote audit focused on processing under this DPA, subject to confidentiality, reasonable notice, scope limitations, and reimbursement of CapConnect's reasonable costs. On-site audits are permitted only where legally required or where a material, unresolved compliance concern cannot reasonably be

addressed remotely.

Audits may not compromise other customers, security, privileged information, or CapConnect trade secrets.

12 12. U.S. State Privacy Terms

Where applicable, CapConnect will:

- process Personal Data only for the limited and specified purposes stated in the Agreement;
- not sell or share Personal Data received from Customer except as permitted by law and the Agreement;
- not retain, use, or disclose such data outside the direct business relationship except as legally permitted;
- provide the same level of privacy protection required of service providers or contractors;
- notify Customer if CapConnect determines it can no longer meet applicable obligations; and
- permit Customer to take reasonable steps to stop and remediate unauthorized use.

13 13. International Transfers

Where Personal Data subject to transfer restrictions is transferred to a country not recognized as providing adequate protection, the parties incorporate the applicable standard contractual clauses or other lawful transfer mechanism.

For transfers subject to the European Economic Area Standard Contractual Clauses, the parties will complete the appropriate controller-to-processor or processor-to-processor module, as applicable. CapConnect's subprocessor list and Security Addendum form the relevant annexes to the extent appropriate.

14 14. Conflict

If this DPA conflicts with the Agreement regarding processing of Personal Data, this DPA controls. The Agreement continues to govern all other matters.

Questions about this document may be sent to legal@capconnectsolutions.com.