CA Solutions LLC

AI Agents · Web & Software · Workflow & CRM Automation · Secure RAG & Knowledge Systems · Communications Automation

Data Processing Addendum

Governs processing of personal data under the Master Services Agreement (US & Canada)

Document Version: 1.0 | **Template Effective Date:** June 2, 2026

Prepared for: CA Solutions LLC

Governing Law: State of Wyoming, United States

Markets Covered: United States & Canada

CA Solutions LLC · 30 N Gould St Ste R # 45751, Sheridan, WY 82801, United States
info@ca-solutions.group · +1 (716) 347-9866 · ca-solutions.group

> This Data Processing Addendum (“DPA”) supplements and forms part of the Master Services Agreement (“MSA”) between CA Solutions LLC and the Client. It governs CA Solutions’ processing of Client Personal Data when CA Solutions acts as a processor / service provider. If this DPA conflicts with the MSA on data-protection matters, this DPA controls.

1. DPA Metadata

Processor / Service Provider	CA Solutions LLC, 30 N Gould St Ste R # 45751, Sheridan, WY 82801
Controller / Business (Client)	`[CLIENT LEGAL NAME & ADDRESS]`
Effective Date	`[DATE]`
Related Agreement	MSA dated `[DATE]`
Related SOWs	`[SOW number(s)]`

2. Definitions

“Controller” means the entity that determines the purposes and means of processing Personal Data.

“Processor” means the entity that processes Personal Data on behalf of the Controller.

“Business” and **“Service Provider”** have the meanings given under the California Consumer Privacy Act, as amended by the CPRA (collectively, “CCPA”), and analogous U.S. state privacy laws.

“Personal Information” and **“Personal Data”** mean information relating to an identified or identifiable individual or household, as defined under applicable Data Protection Laws; both terms are used interchangeably in this DPA.

“Sensitive Personal Information” means the categories of sensitive or special data defined under applicable Data Protection Laws (e.g., government identifiers, financial account information, precise geolocation, health data, biometric data, racial/ethnic origin, and similar).

“Regulated Data” means data subject to heightened legal protection (e.g., PHI, payment-card data, consumer financial data, children’s data).

“Client Personal Data” means Personal Data that CA Solutions processes on Client’s behalf under the MSA.

“Subprocessor” means a third party engaged by CA Solutions to process Client Personal Data.

“Security Incident” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data processed by CA Solutions.

“Data Protection Laws” means all privacy and data-protection laws applicable to the processing, including U.S. state comprehensive privacy laws (such as the CCPA and the comprehensive laws of Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, and other states as enacted), the U.S. HIPAA and GLBA where applicable, Canada’s PIPEDA, applicable provincial private-sector privacy laws, and Quebec’s Law 25.

3. Roles of the Parties

As between the parties, Client is the Controller / Business and CA Solutions is the Processor / Service Provider with respect to Client Personal Data. Where Client is itself a processor/service provider for a third-party controller, CA Solutions acts as a sub-processor and the parties' obligations flow accordingly. CA Solutions does not determine the purposes or means of processing Client Personal Data except as necessary to provide the Services or comply with law.

4. Scope and Duration of Processing

CA Solutions processes Client Personal Data for the duration of the MSA and applicable SOWs and until return or deletion under Section 21. Processing details are set out in Exhibit A.

5. Nature and Purpose of Processing

CA Solutions processes Client Personal Data solely to provide the Services described in the MSA and SOWs (e.g., building and operating websites, AI agents, automations, CRM workflows, RAG/knowledge systems, software, and communications workflows) and as otherwise instructed by Client in writing.

6. Categories of Data Subjects

`[e.g., Client customers, prospects, contacts, employees, end users — as specified in Exhibit A.]`

7. Categories of Personal Data

`[e.g., identifiers, contact data, account data, commercial data, communications data — as specified in Exhibit A.]`

8. Sensitive or Regulated Data

CA Solutions will not process Sensitive Personal Information or Regulated Data unless expressly authorized in a SOW and, for PHI, under an executed Business Associate Agreement. Absent such authorization, Client must not submit such data.

9. Processing Instructions

CA Solutions will process Client Personal Data only on Client's documented instructions (including the MSA, SOWs, and this DPA), unless required by law, in which case CA Solutions will inform Client unless legally prohibited. CA Solutions will promptly inform Client if, in its opinion, an instruction violates Data Protection Laws.

10. Restrictions on Processing

CA Solutions will not retain, use, or disclose Client Personal Data for any purpose other than performing the Services, or as otherwise permitted by Data Protection Laws, and will not combine Client Personal Data with data from other sources except as permitted by the CCPA and other Data Protection Laws.

11. Sale, Sharing, and Targeted Advertising Restrictions

CA Solutions will not “sell” or “share” Client Personal Data, and will not process it for cross-context behavioral advertising or targeted advertising, as those terms are defined under the CCPA and other U.S. state privacy laws. CA Solutions certifies that it understands and will comply with these restrictions.

12. AI Processing Restrictions

12.1 AI Use Cases

AI processing of Client Personal Data is limited to the use cases described in the applicable SOW and Exhibit E.

12.2 Model Training Prohibition

CA Solutions will not use Client Personal Data to train, fine-tune, or improve any third-party foundation model, and will not permit Subprocessors to do so, except with Client’s express written authorization. Where available, CA Solutions configures AI Subprocessors to disable training on Client data and to minimize retention.

12.3 Prompt and Output Handling

Prompts, retrieved content, and outputs containing Client Personal Data are handled as Client Personal Data under this DPA.

12.4 AI Subprocessors

AI providers used to process Client Personal Data are Subprocessors and are listed in Exhibit C, subject to Section 16.

12.5 Human Review

Where the Services support consequential decisioning, Client is responsible for human review and oversight as described in MSA Section 10.

12.6 Automated Decision-Making Restrictions

CA Solutions does not make automated decisions producing legal or similarly significant effects about individuals. If Client configures the Services to do so, Client is responsible for required notices, consent, assessments, and individual rights (including under Quebec Law 25 and U.S. state profiling rules).

13. Confidentiality

CA Solutions will ensure that personnel authorized to process Client Personal Data are bound by confidentiality obligations and process the data only as instructed.

14. Security Measures

CA Solutions will implement and maintain appropriate technical and organizational measures designed to protect Client Personal Data, including, as applicable:

1. **Access Controls** restricting access to authorized personnel.
2. **Authentication**, including multi-factor authentication for administrative access.
3. **Encryption** in transit and, where supported, at rest.
4. **Logging** of relevant access and security events.
5. **Least Privilege** permissioning.
6. **Secure Development** practices.
7. **Vulnerability Management**, including patching and remediation.
8. **Incident Response** procedures.
9. **Backups** appropriate to the Services.
10. **Vendor Review** of Subprocessors.

Full measures are detailed in Exhibit B. CA Solutions may update measures provided protection is not materially diminished.

15. (Reserved)

Security measures are addressed in Section 14 and Exhibit B.

16. Subprocessors

16.1 Approved Subprocessors

Client authorizes CA Solutions to engage the Subprocessors listed in Exhibit C.

16.2 Subprocessor Notice

CA Solutions will give Client at least `[NUMBER]` days' notice (by email or an updated list) before adding or replacing a Subprocessor that processes Client Personal Data.

16.3 Objection Process

Client may object on reasonable data-protection grounds within the notice period; the parties will work in good faith to resolve the objection, and if not resolved, Client may terminate the affected Services.

16.4 Flow-Down Obligations

CA Solutions will impose data-protection obligations on Subprocessors that are no less protective than this DPA and remains responsible for Subprocessors' performance.

16.5 Subprocessor List

A current Subprocessor list is maintained in Exhibit C and made available to Client on request.

17. International Transfers

17.1 Transfer Locations

CA Solutions is based in the United States and may process Client Personal Data in the United States and other jurisdictions where its Subprocessors operate (see Exhibit D).

17.2 Transfer Mechanisms

For transfers subject to Data Protection Laws (including transfers of Canadian personal information), the parties will implement appropriate contractual, organizational, and technical measures, and Client will provide required cross-border transparency to individuals (including under PIPEDA and Quebec Law 25).

17.3 Transfer Impact Assessments

CA Solutions will provide reasonable information to assist Client with transfer or privacy impact assessments where required (including Quebec Law 25 PIAs for transfers outside Quebec).

17.4 Government Access Requests

If CA Solutions receives a legally binding government request for Client Personal Data, it will, unless legally prohibited, notify Client and seek to redirect the request to Client.

18. Assistance with Privacy Rights Requests

Taking into account the nature of the processing, CA Solutions will provide reasonable assistance to enable Client to respond to verified individual requests to access, correct, delete, port, restrict, opt out of sale/sharing/targeted advertising, limit use of sensitive data, or object to processing, as required by Data Protection Laws. If CA Solutions receives such a request directly, it will, where permitted, refer the individual to Client.

19. Assistance with DPIAs, PIAs, and Assessments

CA Solutions will provide reasonable assistance and information to support Client's data-protection impact assessments, privacy impact assessments (including Quebec Law 25 PIAs), and consultations with regulators, to the extent relating to CA Solutions' processing.

20. Security Incident Notification

20.1 Notification Timing

CA Solutions will notify Client without undue delay, and in any event within `[e.g., 72]` hours, after becoming aware of a Security Incident affecting Client Personal Data within its control.

20.2 Required Information

The notice will include, to the extent known, the nature of the incident, categories and approximate number of individuals and records affected, likely consequences, and measures taken or proposed.

20.3 Investigation

CA Solutions will investigate the incident and provide reasonable updates.

20.4 Mitigation

CA Solutions will take reasonable steps to mitigate and remediate the incident.

20.5 Client Notifications

Client is responsible for determining whether and how to notify individuals, regulators, or others, and CA Solutions will reasonably assist. Notification is not an acknowledgment of fault.

21. Return or Deletion of Data

On expiry or termination of the Services, or on Client’s written request, CA Solutions will return or delete Client Personal Data within a reasonable period and certify deletion on request, subject to Section 22.

22. Retention and Backup Exceptions

CA Solutions may retain Client Personal Data to the extent and for the period required by law, in routine backups until overwritten in the ordinary course, and as needed for security, audit, and dispute-resolution purposes, in each case continuing to protect it under this DPA.

23. Audits and Compliance Information

On reasonable prior written notice, no more than once per year (absent a Security Incident or legal requirement), and subject to confidentiality, CA Solutions will make available information reasonably necessary to demonstrate compliance with this DPA, which may include responses to a reasonable security questionnaire or available third-party reports. On-site audits, if any, will be at Client’s expense, scheduled to minimize disruption.

24. Records of Processing

CA Solutions will maintain records of its processing activities as required by Data Protection Laws.

25. De-Identified and Aggregated Data

CA Solutions may create and use de-identified or aggregated data derived from Client Personal Data for security, reliability, and service-improvement purposes, provided it does not attempt to re-identify the data, maintains the data in de-identified form, and contractually obligates recipients to the same, consistent with Data Protection Laws.

26. U.S. State Privacy Law Terms

26.1 CCPA/CPRA Service Provider Terms

CA Solutions is a Service Provider and will: process Personal Information only for the business purposes specified; not sell or share it; not retain, use, or disclose it outside the direct business relationship or for any purpose other than the Services; not combine it with other data except as permitted; and comply with applicable CCPA obligations. CA Solutions certifies it understands and will comply with these restrictions.

26.2 Controller/Processor Terms

For states using controller/processor terminology (e.g., Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, and others as enacted), CA Solutions acts as Processor and will adhere to Client’s instructions, assist with security and individual rights, ensure confidentiality, engage Subprocessors under flow-down terms, and make available information to demonstrate compliance.

26.3 Sensitive Data Terms

CA Solutions will process Sensitive Personal Information only as instructed and only where authorized in a SOW.

26.4 Opt-Out Assistance

CA Solutions will assist Client in honoring opt-outs of sale, sharing, targeted advertising, and certain profiling, and will not process opted-out data for restricted purposes.

27. Canadian Privacy Law Terms

27.1 PIPEDA

Where PIPEDA applies, CA Solutions will process personal information consistent with Client’s instructions and provide a comparable level of protection while the information is in its custody, supporting Client’s accountability, safeguards, and openness obligations.

27.2 Provincial Private Sector Privacy Laws

Where provincial private-sector privacy laws apply (e.g., Alberta, British Columbia, Quebec), CA Solutions will support Client's compliance to the extent relating to its processing.

27.3 Quebec Law 25 Considerations

Where Quebec's Law 25 applies, CA Solutions will: process personal information only as instructed; assist Client with privacy impact assessments (including for transfers outside Quebec); support Client's confidentiality, retention, and individual-rights obligations (including access, correction, de-indexing, and data portability); notify Client of confidentiality incidents to support Client's reporting obligations; and support Client's transparency regarding automated decision-making where applicable.

27.4 Cross-Border Transparency

Client is responsible for informing individuals that their personal information may be processed outside their province or Canada, as required.

28. Sector-Specific Addenda

28.1 HIPAA Business Associate Agreement Reference

If CA Solutions processes PHI on Client's behalf, the parties will execute a separate Business Associate Agreement, which governs PHI and controls over this DPA as to PHI.

28.2 GLBA Safeguards Reference

Where Client is a financial institution subject to the Gramm-Leach-Bliley Act, CA Solutions will maintain safeguards reasonably designed to support Client's obligations under the GLBA Safeguards Rule for data within its control.

28.3 Payment Card Data Exclusion

CA Solutions does not store, process, or transmit cardholder data and is not a PCI-DSS service provider unless expressly agreed in a SOW. Payment processing is handled by Client's third-party processors.

28.4 Children's Data Addendum

CA Solutions does not knowingly process children's personal information. If a SOW involves children's data, the parties will agree additional COPPA and applicable state/provincial controls before any such processing.

29. Liability and Indemnity Relationship to MSA

The limitations of liability and indemnification provisions in the MSA apply to this DPA and to claims arising from processing of Client Personal Data, except to the extent a limitation is prohibited by Data Protection Laws.

30. Term and Termination

This DPA is effective for as long as CA Solutions processes Client Personal Data under the MSA and survives termination until return or deletion is complete.

31. Conflict

In case of conflict between this DPA and the MSA regarding the processing of Client Personal Data, this DPA controls. In case of conflict between this DPA and an executed BAA regarding PHI, the BAA controls as to PHI.

32. Exhibits

Exhibit A — Processing Details

Subject Matter	`[Provision of the Services under the MSA/SOWs]`
Duration	Term of the MSA/SOWs plus retention period
Nature & Purpose	`[Describe]`
Categories of Data Subjects	`[Describe]`
Categories of Personal Data	`[Describe]`
Sensitive / Regulated Data	`[None unless authorized]`
Frequency	`[Continuous / batch]`

Exhibit B — Security Measures

Detailed technical and organizational measures: access controls and least privilege; MFA for administrative access; encryption in transit and (where supported) at rest; secrets management; logging and monitoring; vulnerability and patch management; secure SDLC; backups; subprocessor security review; and documented incident response. `[Attach detailed measures specific to the engagement.]`

Exhibit C — Subprocessor List

Subprocessor	Service	Processing Location	Data Categories
`[Name]`	`[e.g., cloud hosting]`	`[Location]`	`[Categories]`
`[Name]`	`[e.g., AI/model API]`	`[Location]`	`[Categories]`
`[Name]`	`[e.g., CRM / messaging]`	`[Location]`	`[Categories]`

Exhibit D — Transfer Mechanism

`[Describe transfer locations and mechanisms/safeguards for cross-border transfers, including any Canada-to-US transfer transparency and safeguards.]`

Exhibit E — AI Processing Details

AI Use Case	`[Describe]`
Models / Providers	`[List]`
Training on Client Data	Disabled unless expressly authorized
Retention by AI Provider	`[Minimized / per provider terms]`
Human Review	`[Where required]`

33. Signature Blocks

CA SOLUTIONS LLC (Processor / Service Provider)

Signature

Name / Title

Date

`[CLIENT LEGAL NAME]` (Controller / Business)

Signature

Name / Title

Date

> **Attorney note (current as of June 2026):** Twenty U.S. states have enacted comprehensive privacy laws; confirm which apply based on Client's thresholds and update Section 26 accordingly. Quebec's Law 25 is fully in force (data portability effective Sept. 22, 2024) and carries a private right of action and administrative monetary penalties; PIAs are required for transfers outside Quebec. Confirm the federal Canadian framework (PIPEDA / any successor legislation) at execution.