

AxiaForce

DATA PROCESSING ADDENDUM

AxiaForce, Inc.

Version 1.0 | Effective Date: October 12, 2026

This Data Processing Addendum ("DPA") describes the privacy and data-protection obligations that apply when AxiaForce, Inc. Processes Personal Data on behalf of a customer in connection with the AxiaForce Services. It is incorporated into and forms part of the applicable Agreement.

1. Scope and Incorporation

This Data Processing Addendum ("DPA") forms part of the agreement governing Customer's use of the AxiaForce Services (the "Agreement") and applies where AxiaForce Processes Customer Personal Data on behalf of Customer.

If there is a conflict between this DPA and the Agreement regarding Processing of Customer Personal Data, this DPA controls. If applicable Standard Contractual Clauses or another mandatory transfer mechanism conflicts with this DPA, the mandatory transfer mechanism controls for the affected Processing.

2. Definitions

"Applicable Data Protection Law" means any privacy, data-protection, or data-security law applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the GDPR, UK GDPR, Swiss Federal Act on Data Protection, CCPA/CPRA, and other U.S. state privacy laws.

"Customer Personal Data" means Personal Data contained in Customer Data and Processed by AxiaForce on behalf of Customer.

"Controller," "Processor," "Business," "Service Provider," "Contractor," "Personal Data," "Process," "Processing," "Data Subject," and "Supervisory Authority" have the meanings assigned by Applicable Data Protection Law.

"Subprocessor" means a third party engaged by AxiaForce to Process Customer Personal Data on behalf of Customer in connection with the Services.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

3. Roles of the Parties

Where Customer determines the purposes and means of Processing Customer Personal Data, Customer acts as Controller/Business and AxiaForce acts as Processor/Service Provider.

Where Customer acts as a Processor or Service Provider on behalf of another Controller or Business, AxiaForce acts as Customer's subprocessor or subcontractor to the extent applicable.

Each party will comply with the obligations applicable to it under Applicable Data Protection Law.

4. Customer Instructions and Responsibilities

Customer instructs AxiaForce to Process Customer Personal Data as necessary to provide, secure, support, maintain, and improve the Services in accordance with the Agreement, Customer's configuration and use of the Services, this DPA, and any additional lawful written instructions agreed by the parties.

Customer is responsible for the lawfulness of its instructions and for obtaining any notices, consents, permissions, and legal bases required to collect and provide Customer Personal Data to AxiaForce.

If AxiaForce reasonably believes an instruction violates Applicable Data Protection Law, AxiaForce may notify Customer and suspend the affected Processing until the parties resolve the issue.

5. Nature, Purpose, and Duration of Processing

AxiaForce Processes Customer Personal Data to provide AI-enabled software, agentic workflows, integrations, communications, reporting, automation, support, security, and related functionality selected or configured by Customer.

Processing may include collection, access, organization, hosting, storage, retrieval, consultation, analysis, transformation, transmission, generation of outputs, synchronization, deletion, and other operations necessary to provide the Services.

Processing continues for the term of the Agreement and any limited post-termination period described in this DPA or required by law.

6. AI and Automated Processing

Customer acknowledges that the Services may use artificial intelligence, machine learning, large language models, automated systems, and autonomous or semi-autonomous agents to Process Customer Personal Data for Customer-configured purposes.

AxiaForce may transmit Customer Personal Data to authorized AI/model providers acting as Subprocessors where necessary to provide enabled functionality.

AxiaForce will not use Customer Personal Data to train generalized models for unrelated third-party use unless Customer expressly authorizes such use or the practice is expressly disclosed in an applicable agreement.

Customer remains responsible for determining whether its use of AI-enabled functionality is lawful and appropriate for its use case, including any required human review or notice obligations.

7. Confidentiality

AxiaForce will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations and access Customer Personal Data only as necessary for their assigned responsibilities.

8. Security Measures

AxiaForce will maintain appropriate administrative, technical, and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

Each AxiaForce customer tenant is provisioned with its own separate database. Customer Data from different tenants is not stored together in a shared customer database. Tenant-specific authorization controls, credentials, application context, and access boundaries are designed to restrict each tenant to its own database, configuration, users, integrations, and Customer Data.

The measures are described at a high level in Annex 2 and may evolve as AxiaForce improves the Services, provided that the overall level of protection is not materially diminished during an active subscription term.

9. Personal Data Breach

AxiaForce will notify Customer without undue delay after becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data.

As information becomes reasonably available, AxiaForce will provide information sufficient to assist Customer in meeting applicable breach-notification obligations, including the nature of the incident, categories of affected data where known, mitigation measures taken or planned, and a point of contact for follow-up.

AxiaForce's notification of an incident is not an admission of fault or liability.

10. Data Subject Requests

Taking into account the nature of the Processing, AxiaForce will provide commercially reasonable assistance to Customer in responding to requests from Data Subjects exercising rights under Applicable Data Protection Law.

If AxiaForce receives a request directly from a Data Subject concerning Customer Personal Data, AxiaForce may direct the requester to Customer unless Applicable Data Protection Law requires AxiaForce to respond directly.

Customer is responsible for determining whether and how to respond to a request.

11. Privacy Impact Assessments and Regulatory Cooperation

Taking into account the nature of the Processing and information available to AxiaForce, AxiaForce will provide commercially reasonable assistance with data-protection impact assessments, prior consultations, and inquiries from Supervisory Authorities to the extent required by Applicable Data Protection Law and related to AxiaForce's Processing of Customer Personal Data.

12. Subprocessors

Customer provides general authorization for AxiaForce to engage Subprocessors to Process Customer Personal Data.

AxiaForce will maintain a current list of material Subprocessors used for the Services and will make that list available to Customer upon reasonable request. AxiaForce is not required to publish its complete Subprocessor list publicly.

AxiaForce will require each Subprocessor to protect Customer Personal Data under written obligations that provide materially equivalent data-protection protections appropriate to the services performed.

Where reasonably practicable, AxiaForce will provide advance notice of a new material Subprocessor using the notice mechanisms described in the Agreement. Customer may raise a reasonable, documented data-protection objection within fifteen (15) days after notice. The parties will work in good faith to address the concern. If no commercially reasonable resolution is available, AxiaForce may offer an alternative configuration or Customer may discontinue the affected portion of the Services without affecting unrelated Services.

13. International Processing and Transfers

AxiaForce is a United States-based service provider. Customer Personal Data may be Processed in the United States and other jurisdictions where AxiaForce or its authorized Subprocessors operate.

The international-transfer provisions in this DPA apply only to the extent required by Applicable Data Protection Law for the relevant Customer Personal Data and transfer.

Where Applicable Data Protection Law restricts international transfers, the parties will rely on an applicable lawful transfer mechanism, including an adequacy decision, the EU Standard Contractual Clauses, the UK International Data Transfer Addendum or other recognized safeguards, as applicable.

AxiaForce does not guarantee country-specific or regional data residency unless expressly agreed in writing.

14. European Economic Area - Standard Contractual Clauses

Only to the extent required by Applicable Data Protection Law for a relevant transfer of Customer Personal Data subject to the GDPR, and where no applicable adequacy decision or other lawful transfer mechanism applies, the European Commission Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 ("EU SCCs") are incorporated into this DPA by reference.

Module Two (Controller to Processor) applies where Customer is a Controller and AxiaForce is a Processor. Module Three (Processor to Processor) applies where Customer is a Processor and AxiaForce is a subprocessor.

The Annexes to this DPA will serve as the corresponding annex information for the EU SCCs. Docking is permitted. Optional language will apply only where expressly stated in this DPA or required by law.

15. United Kingdom

Only to the extent required by Applicable Data Protection Law for a relevant restricted transfer subject to the UK GDPR, the applicable EU SCCs as incorporated into this DPA will be supplemented by the then-current UK International Data Transfer Addendum issued by the UK Information Commissioner's Office, or another legally recognized UK transfer mechanism, as applicable.

References in the EU SCCs will be interpreted as necessary to give effect to UK data-protection law.

16. Switzerland

Only to the extent required by Applicable Data Protection Law for a relevant transfer subject to Swiss data-protection law, the EU SCCs are incorporated with adaptations required by the Swiss Federal Act on Data Protection, including references to the competent Swiss authority and recognition of Swiss Data Subjects as applicable.

17. United States State Privacy Laws

To the extent Customer Personal Data is subject to a U.S. state privacy law and AxiaForce acts as a Service Provider, Contractor, or Processor, AxiaForce will Process Customer Personal Data only for the business purposes specified in the Agreement and Customer's documented instructions.

AxiaForce will not sell or share Customer Personal Data as those terms are defined by Applicable Data Protection Law, and will not retain, use, or disclose Customer Personal Data outside the direct business relationship with Customer except as permitted by Applicable Data Protection Law and the Agreement.

AxiaForce will not combine Customer Personal Data with Personal Data received from or on behalf of another person or collected from AxiaForce's own interaction with an individual except where permitted by Applicable Data Protection Law.

18. Government and Law-Enforcement Requests

If AxiaForce receives a legally binding request from a government or law-enforcement authority for Customer Personal Data, AxiaForce will, where legally permitted, notify Customer before disclosure.

AxiaForce will review the request, disclose only the information legally required, and where appropriate and legally available, use reasonable efforts to challenge requests that are facially unlawful or materially overbroad.

If notice is legally prohibited, AxiaForce will use reasonable efforts to preserve Customer's interests to the extent permitted by law.

19. Return and Deletion

Customer acknowledges that the Services are designed to integrate with and process data from Customer-controlled systems and that Customer is responsible for maintaining its own systems of record and copies of Customer Data.

Upon expiration or termination of the applicable Services, AxiaForce will cease Processing Customer Personal Data except as necessary to complete termination activities, comply with applicable law, maintain security or audit records, or as otherwise permitted by the Agreement.

To the extent Customer Personal Data remains in AxiaForce active systems after termination, AxiaForce will delete or anonymize such data within sixty (60) days, unless a different period is required by applicable law or agreed in writing. Customer Personal Data contained in encrypted backups may remain for up to an additional ninety (90) days in accordance with normal backup cycles and will remain protected from ordinary use.

AxiaForce is not required to create a new export, migration package, or data-delivery mechanism where Customer already maintains the applicable data in Customer-controlled systems or where the applicable Service does not provide export functionality.

Nothing in this Section requires AxiaForce to provide Customer with AxiaForce proprietary technology, internal system data, platform configurations, reusable workflows, prompts, models, algorithms, scoring methodologies, internal telemetry,

or other AxiaForce intellectual property.

To the extent Applicable Data Protection Law requires return of Customer Personal Data, AxiaForce will provide such Personal Data using commercially reasonable means and available functionality, but is not required to disclose AxiaForce proprietary materials or create a custom export capability unless separately agreed in writing.

AxiaForce may retain limited records where required for legal, security, fraud-prevention, dispute, accounting, or compliance purposes.

20. Demonstration of Compliance and Audits

Upon reasonable request, AxiaForce will make available information reasonably necessary to demonstrate compliance with this DPA, which may include security documentation, questionnaires, audit summaries, certifications when available, or other compliance materials.

Customer will first use available documentation and remote review processes before requesting an on-site audit.

Where Applicable Data Protection Law requires an audit and available documentation is insufficient, Customer may conduct or appoint an independent auditor to conduct an audit no more than once in any twelve-month period, on reasonable advance notice, during normal business hours, without disrupting AxiaForce operations, and subject to confidentiality and security requirements.

Customer will bear its audit costs unless the audit identifies a material violation of this DPA by AxiaForce.

21. Customer-Controlled Integrations

Where Customer enables an integration with a third-party service, Customer instructs AxiaForce to transmit or make Customer Personal Data available to that third party as necessary to provide the integration.

Customer is responsible for its relationship with Customer-selected third parties and for ensuring it has authority to direct the transfer.

Once Customer Personal Data is received by a third party acting independently of AxiaForce, that third party's privacy and security practices may govern its Processing.

22. Assignment and Change of Control

This DPA may be assigned, transferred, or assumed together with the Agreement in accordance with the assignment and change-of-control provisions of the Agreement, including in connection with a merger, acquisition, corporate reorganization, financing transaction, or sale of all or substantially all of the relevant business or assets.

No separate Customer consent is required solely because this DPA transfers with the Agreement, provided that the successor assumes AxiaForce's applicable obligations under this DPA and Applicable Data Protection Law.

Any transfer of Customer Personal Data in connection with such a transaction remains subject to this DPA and Applicable Data Protection Law.

23. Updates to this DPA

AxiaForce may update this DPA to reflect changes in law, regulatory guidance, transfer mechanisms, security practices, or the Services.

AxiaForce will provide notice of material changes using the notice mechanisms described in the Agreement. Updates required by law or that do not materially diminish protections for Customer Personal Data may take effect on the stated effective date.

If a change materially diminishes contractual protections for Customer Personal Data during a committed term, Customer may notify AxiaForce of a reasonable data-protection objection within thirty (30) days after notice, and the parties will work in good faith to address the concern.

24. General

This DPA terminates automatically when AxiaForce no longer Processes Customer Personal Data on Customer's behalf, except for provisions that by their nature survive termination.

Except as modified by this DPA, the Agreement remains in full force and effect.

25. Annex 1 - Details of Processing

Subject Matter: Processing of Customer Personal Data to provide the AxiaForce Services selected or configured by Customer.

Duration: For the term of the Agreement plus limited post-termination retention described in this DPA.

Nature and Purpose: Hosting, storage, retrieval, analysis, generation, automation, synchronization, communications, workflow execution, integration, support, security, monitoring, reporting, and related operations necessary to provide the Services.

Categories of Data Subjects: Customer personnel; authorized users; applicants and candidates; prospects and leads; Customer customers and end users; business contacts; vendors; contractors; collaborators; and other individuals whose Personal Data Customer submits to the Services.

Categories of Personal Data: Business contact information; account and authentication data; CRM data; recruiting and candidate information; employment-related information submitted by Customer; email and calendar data; communications; call recordings and transcripts where enabled; files and documents; workflow data; support data; identifiers; usage and device metadata; integration data; and other Personal Data submitted or connected by Customer.

Sensitive Data: The Services are not intended for unrestricted Processing of highly sensitive or regulated data unless the applicable Service, Order Form, or written agreement expressly supports such Processing. Customer is responsible for ensuring that any sensitive data it submits is permitted.

Frequency: Continuous or as initiated/configured by Customer through use of the Services.

26. Annex 2 - Technical and Organizational Measures

AxiaForce maintains security measures appropriate to the nature of the Services and risks presented by the Processing.

Tenant Data Isolation. Each AxiaForce customer tenant is provisioned with its own separate database. Customer Data from different tenants is not stored together in a shared customer database. Tenant-specific authorization controls, credentials, application context, and access boundaries are designed to restrict each tenant to its own database, configuration, users, integrations, and Customer Data. Database-level separation is supplemented by application-level authorization and access controls designed to prevent cross-tenant access.

Additional measures include, as applicable: identity and access controls; least-privilege access; multi-factor authentication for privileged access; encryption in transit and at rest where technically supported; secrets and credential management; logging and monitoring; vulnerability and patch management; secure software-development practices; backup and recovery controls; incident-response procedures; personnel confidentiality obligations; vendor and Subprocessor review; access revocation procedures; and measures designed to protect AI-enabled and agentic workflows from unauthorized access or execution.

Security controls may evolve over time as technologies and risks change, provided that AxiaForce will not materially diminish the overall security of the Services during an active subscription term.

27. Annex 3 - Subprocessors and Transfer Information

AxiaForce will maintain its current material Subprocessor list separately from this DPA so that infrastructure and provider changes do not require republication of the complete DPA.

The Subprocessor list is maintained as confidential operational and compliance information and will be made available to Customer upon reasonable request. AxiaForce is not required to publish its complete provider stack or Subprocessor list publicly.

The list will identify, as appropriate, the provider, purpose or service category, and primary Processing location or region where reasonably available.

Customer's use of the Services after the applicable objection period for a notified new material Subprocessor constitutes authorization of that Subprocessor, subject to Customer's rights under the Subprocessors section of this DPA.

END OF DATA PROCESSING ADDENDUM