Actia AI

Data Processing Addendum

Effective Date: June 1, 2026

This Data Processing Addendum ("DPA") forms part of the Actia AI Terms of Use or other written agreement governing access to and use of the Services between Actia LLC, doing business as Actia AI ("Actia AI," "Actia," "we," "our," or "us"), and the customer that uses the Services ("Customer," "you," or "your").

This DPA applies where Actia processes Personal Data on behalf of Customer in connection with the Services. Capitalized terms not defined in this DPA have the meanings given to them in the Terms of Use.

1. Purpose and Scope

Actia provides a hosted business AI-agent platform that enables Customer to configure AI agents, communication channels, business-application connectors, knowledge sources, workflows, messages, and related platform functionality.

In providing the Services, Actia may process Personal Data contained in Customer Data on behalf of Customer. This DPA sets out the parties' data protection obligations for that processing.

This DPA applies only to Personal Data processed by Actia on behalf of Customer. It does not apply to personal information that Actia processes as an independent controller or business, such as account administration, billing, website analytics, sales, marketing, security, or support information, which is addressed in the Actia AI Privacy Policy.

2. Definitions

"Applicable Data Protection Laws" means privacy, data protection, and data security laws applicable to the processing of Personal Data under this DPA, which may include the GDPR, UK GDPR, Data Protection Act 2018, Swiss data protection law, the California Consumer Privacy Act as amended by the California Privacy Rights Act, and other applicable privacy laws.

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

"Customer Data" has the meaning given in the Terms of Use and includes Personal Data submitted to, generated through, processed by, or made available to the Services by or on behalf of Customer.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

"GDPR" means Regulation (EU) 2016/679.

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by Actia on behalf of Customer as part of Customer Data.

“Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed by Actia on behalf of Customer.

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

“Restricted Transfer” means a transfer of Personal Data from the European Economic Area, United Kingdom, or Switzerland to a country that is not recognized as providing an adequate level of protection under Applicable Data Protection Laws.

“Services” means the Actia AI services described in the Terms of Use.

“Subprocessor” means a third party engaged by Actia to process Personal Data on behalf of Customer in connection with the Services.

“UK GDPR” means the GDPR as incorporated into United Kingdom law.

3. Roles of the Parties

For Personal Data processed by Actia on behalf of Customer under this DPA, Customer is the Controller and Actia is the Processor, unless Applicable Data Protection Laws use different terminology.

For purposes of the California Consumer Privacy Act, as amended, Actia acts as a service provider or contractor with respect to Personal Information it processes on behalf of Customer, and Customer acts as the business, unless the parties agree otherwise in writing.

Customer is responsible for determining the purposes and means of processing Customer Data, including what Personal Data is provided to the Services, how AI agents are configured, which business applications are connected, what workflows are enabled, and what notices, consents, legal bases, and safeguards are required.

Actia will process Personal Data only as described in this DPA, the Terms of Use, applicable orders, Customer’s documented instructions, and Applicable Data Protection Laws.

4. Customer Instructions

Customer instructs Actia to process Personal Data as necessary to provide, maintain, secure, support, monitor, troubleshoot, and improve the Services; to perform obligations under the Terms of Use; to prevent or address misuse, fraud, security incidents, or technical issues; to comply with applicable law; and as otherwise documented by Customer through platform configuration, support requests, orders, or written instructions.

Actia will not process Personal Data for purposes outside Customer’s documented instructions unless required by law. If Actia is required by law to process Personal Data outside Customer’s instructions, Actia will inform Customer of that legal requirement before processing unless prohibited by law.

Actia will promptly inform Customer if Actia believes an instruction violates Applicable Data Protection Laws.

5. Details of Processing

The details of processing are set out in Annex 1 to this DPA.

6. Confidentiality

Actia will ensure that persons authorized to process Personal Data are subject to appropriate confidentiality obligations or professional or statutory obligations of confidentiality.

Actia will limit access to Personal Data to personnel and service providers who need access to provide, secure, support, or maintain the Services.

7. Security Measures

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

The security measures are described in Annex 2 to this DPA. Customer acknowledges that security measures may be updated from time to time, provided that Actia does not materially reduce the overall level of protection for Personal Data during an active subscription term.

Customer is responsible for securing its own systems, accounts, credentials, devices, networks, users, connected applications, access permissions, agent configurations, and workflows.

8. Subprocessors

Customer authorizes Actia to engage Subprocessors to process Personal Data in connection with the Services.

Actia will impose data protection obligations on Subprocessors that are no less protective in substance than those imposed on Actia under this DPA, to the extent applicable to the nature of the services provided by the Subprocessor.

Actia remains responsible for the performance of its Subprocessors' obligations as they relate to processing Personal Data on behalf of Customer.

Actia may use categories of Subprocessors that support the Services, such as cloud hosting, database services, AI model services, voice-processing providers, telephony providers, email and messaging infrastructure, analytics, payment processing, customer support, security monitoring, authentication, and system administration. Actia will provide notice of material changes to Subprocessor categories where required by Applicable Data Protection Laws or an applicable agreement.

If Customer objects to a new Subprocessor on reasonable data protection grounds, Customer must notify Actia within a reasonable period after receiving notice. The parties will work in good faith to address the objection. If the objection cannot be resolved, Customer may stop using the affected feature or terminate the affected Services as provided in the Terms of Use.

9. Assistance With Data Subject Requests

Taking into account the nature of the processing, Actia will provide reasonable assistance to Customer, through technical and organizational measures where possible, to help Customer respond to Data Subject requests under Applicable Data Protection Laws.

If Actia receives a request from a Data Subject relating to Personal Data processed on behalf of Customer, Actia may direct the requester to Customer or notify Customer, unless prohibited by law.

Customer is responsible for responding to Data Subject requests where Customer is the Controller or business responsible for the Personal Data.

10. Assistance With Compliance

Taking into account the nature of the processing and information available to Actia, Actia will provide reasonable assistance to Customer with Customer's obligations relating to security, breach notification, data protection impact assessments, and prior consultation with supervisory authorities where required by Applicable Data Protection Laws.

Actia may charge reasonable fees for assistance that is not included in the standard Services, unless the assistance is required due to Actia's breach of this DPA.

11. Personal Data Breach

Actia will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed by Actia on behalf of Customer.

The notice will include available information reasonably required for Customer to meet its breach notification obligations, such as the nature of the breach, categories of affected Personal Data, approximate number of affected Data Subjects where known, likely consequences where known, and measures taken or proposed to address the breach.

Actia's notification of a Personal Data Breach is not an admission of fault or liability.

Customer is responsible for determining whether notice to Data Subjects, regulators, customers, employees, or other third parties is required.

12. Deletion and Return

Upon termination or expiration of the Services, Actia will delete or return Personal Data processed on behalf of Customer in accordance with the Terms of Use, this DPA, applicable platform functionality, and Applicable Data Protection Laws.

Customer is responsible for exporting Customer Data before termination where export functionality is available.

Actia may retain Personal Data to the extent required by law or as necessary for legal, regulatory, security, fraud prevention, dispute resolution, backup, or compliance purposes, provided that retained Personal Data remains subject to appropriate confidentiality and security protections.

Actia may retain aggregated, de-identified, statistical, diagnostic, security, billing, and usage information that does not identify Customer or an identifiable individual.

13. Audits and Compliance Information

Actia will make available information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, security, and operational limitations.

Customer may request reasonable information about Actia's security and data protection practices. Actia may satisfy such requests by providing summaries, security documentation, audit reports, certifications, questionnaires, or other compliance materials.

If Applicable Data Protection Laws require an audit, Customer may request an audit no more than once per year, unless a Personal Data Breach or legal requirement justifies an additional

audit. Audits must be conducted during normal business hours, with reasonable advance notice, in a manner that does not disrupt Actia's operations, compromise security, or expose information relating to other customers.

Customer is responsible for its own audit costs. Actia may charge reasonable fees for audit support unless the audit is required due to Actia's breach of this DPA.

14. International Transfers

Customer acknowledges that Actia operates the Services on a U.S.-first basis and that Actia and its Subprocessors may process Personal Data in the United States and other countries where Actia or its Subprocessors operate.

For Restricted Transfers, the parties will use an appropriate transfer mechanism recognized under Applicable Data Protection Laws, such as the Standard Contractual Clauses, the UK International Data Transfer Addendum, the UK International Data Transfer Agreement, an adequacy decision, or another lawful transfer mechanism.

Where Standard Contractual Clauses are required, the parties agree that the applicable controller-to-processor clauses are incorporated by reference into this DPA and completed as set out in Annex 3, unless the parties execute a separate transfer agreement.

15. California Service Provider and Contractor Terms

To the extent Actia processes Personal Information on behalf of Customer subject to the California Consumer Privacy Act, as amended, Actia will act as a service provider or contractor and agrees that it will not:

(a) sell or share Personal Information processed on behalf of Customer;

(b) retain, use, or disclose Personal Information for any purpose other than the business purposes specified in the Terms of Use, this DPA, Customer's documented instructions, or as otherwise permitted by the CCPA;

(c) retain, use, or disclose Personal Information for a commercial purpose other than the business purposes specified in the agreement with Customer, unless permitted by the CCPA;

(d) retain, use, or disclose Personal Information outside the direct business relationship between Actia and Customer, unless permitted by the CCPA;

(e) combine Personal Information received from or on behalf of Customer with Personal Information received from another source or collected from Actia's own interaction with a consumer, except as permitted by the CCPA.

Actia will comply with applicable obligations under the CCPA and will provide the same level of privacy protection required of service providers or contractors under the CCPA.

Customer has the right to take reasonable and appropriate steps to help ensure that Actia uses Personal Information in a manner consistent with Customer's obligations under the CCPA. Customer may exercise this right through reasonable requests for compliance information as described in this DPA.

Actia will notify Customer if Actia determines that it can no longer meet its obligations under the CCPA. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

16. Sensitive and Regulated Data

Customer must not submit or make available sensitive, regulated, high-risk, or special-category Personal Data to the Services unless Customer has all required legal bases, notices, consents, safeguards, agreements, and authorizations and Actia has expressly agreed in writing to support the applicable data type or regulatory framework.

Customer is responsible for determining whether its use of the Services involves sensitive or regulated data, including health information, financial information, government identifiers, children's data, biometric data, employment data, education records, communications data, or other regulated information.

Actia is not responsible for Customer's decision to process sensitive or regulated data through the Services unless Actia has expressly agreed in writing to support that data type or regulatory framework.

17. AI Processing and Customer Configuration

Customer acknowledges that AI agents may process Personal Data in accordance with Customer's configuration, instructions, connected applications, communication channels, knowledge sources, approval settings, and workflows.

Customer is responsible for ensuring that AI processing is lawful, fair, transparent, and appropriate for the context in which Customer uses the Services. Customer is also responsible for determining whether notices or disclosures are required when individuals interact with AI agents configured by Customer, and Customer must not use the Services in a manner that is deceptive or misleading.

Customer must implement appropriate human review, notices, safeguards, and compliance measures for workflows involving sensitive, regulated, high-impact, or legally significant decisions.

Actia does not use Customer Data to train third-party foundation models unless Customer expressly authorizes such use or the data has been de-identified or aggregated so that it is no longer reasonably associated with Customer or an identifiable individual.

18. Order of Precedence

If there is a conflict between this DPA and the Terms of Use regarding the processing of Personal Data on behalf of Customer, this DPA will control.

If there is a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will control to the extent required by Applicable Data Protection Laws.

19. Term

This DPA remains in effect for as long as Actia processes Personal Data on behalf of Customer.

Annex 1: Details of Processing

Subject Matter

Actia's processing of Personal Data on behalf of Customer in connection with the provision of the Services.

Duration

For the term of Customer's use of the Services and for any additional period during which Actia processes Personal Data in accordance with the Terms of Use, this DPA, retention settings, legal obligations, backup practices, or Customer instructions.

Nature and Purpose of Processing

Actia processes Personal Data to provide, maintain, secure, monitor, support, troubleshoot, and improve the Services; enable AI agents and business workflows; process communications, messages, emails, voice interactions, chat, and messaging content; connect to Customer-authorized business applications; retrieve and use business context; generate outputs; create or update workflow records; provide support; prevent abuse; comply with law; and perform obligations under the Terms of Use.

Types of Personal Data

Depending on Customer's configuration and use of the Services, Personal Data may include:

- names;
- business contact details;
- company affiliation;
- job title;
- account and user identifiers;
- email addresses;
- phone numbers;
- communication content;
- call interaction records;
- email content;
- chat and messaging content;
- customer, prospect, vendor, or staff records;
- business application data;
- task, ticket, appointment, service request, lead, or workflow data;
- notes, summaries, classifications, and AI-generated outputs;
- authentication and access logs;
- IP addresses and device information;
- usage, diagnostic, and security logs;
- other Personal Data submitted to or generated through the Services by or on behalf of Customer.

Categories of Data Subjects

Depending on Customer's use of the Services, Data Subjects may include:

- Customer's employees, contractors, administrators, and authorized users;
- Customer's customers, prospects, leads, vendors, partners, and business contacts;
- individuals who communicate with Customer or Customer's AI agents by phone, email, chat, messaging, or other channels;
- individuals whose information is contained in connected business applications, records, communications, documents, or knowledge sources;
- other individuals whose Personal Data is submitted to or processed through the Services by or on behalf of Customer.

Processing Activities

Processing activities may include collection, creation, organization, structuring, storage, adaptation, retrieval, consultation, use, transmission, disclosure, alignment, combination, restriction, deletion, destruction, analysis, summarization, classification, generation, transformation, and other operations necessary to provide the Services.

Annex 2: Technical and Organizational Measures

Actia will maintain reasonable technical and organizational measures designed to protect Personal Data, which may include:

Access Controls

- user authentication;
- administrative access controls;
- role-based or permission-based access where available;
- least-privilege access principles;
- restricted internal access to Customer Data;
- credential management practices.

Encryption and Transmission Security

- encryption in transit using industry-standard protocols where technically feasible;
- encryption at rest for applicable hosted data stores where technically feasible;
- secure administrative access methods.

System Security

- cloud infrastructure security controls;
- network and application security measures;
- security monitoring;
- vulnerability management practices;
- security review of material platform changes;
- malware and abuse-prevention measures where applicable.

Data Protection and Isolation

- logical separation of customer workspaces or accounts;
- controls designed to prevent unauthorized cross-customer access;
- backup, retention, and recovery practices appropriate to the Services;
- deletion or de-identification practices where applicable.

Personnel and Vendor Controls

- confidentiality obligations for personnel with access to Personal Data;
- access limited to personnel with a business need;
- review of relevant service providers;
- contractual data protection obligations for Subprocessors.
- processes to identify, assess, respond to, and mitigate security incidents;
- escalation and notification procedures;
- remediation tracking where appropriate.

Availability and Resilience

- use of hosted infrastructure designed for availability and resilience;
- backup or recovery practices appropriate to the Services;
- monitoring of service performance and reliability.

Customer acknowledges that specific controls may vary by feature, plan, hosting environment, integration, and technical configuration.

Annex 3: International Transfer Terms

Where required for a Restricted Transfer, the parties agree that the applicable Standard Contractual Clauses are incorporated by reference as follows:

EEA Transfers

For transfers from the European Economic Area, the EU Standard Contractual Clauses approved by the European Commission for controller-to-processor transfers apply.

UK Transfers

For transfers from the United Kingdom, the UK International Data Transfer Addendum or another lawful UK transfer mechanism applies, as applicable.

Swiss Transfers

For transfers from Switzerland, the applicable Standard Contractual Clauses apply with modifications required by Swiss data protection law.

Clause Completion

For purposes of the Standard Contractual Clauses:

- Customer is the data exporter.
- Actia is the data importer.
- The parties' details are set out in the Terms of Use, applicable order, or Customer account information.
- The processing details are set out in Annex 1.
- The technical and organizational measures are set out in Annex 2.
- Subprocessor authorization is general authorization as described in this DPA.
- The governing law and forum are as required by the applicable Standard Contractual Clauses.

If the parties execute separate transfer terms, those terms will control to the extent they conflict with this Annex.