Data Processing Agreement

InsightPlay AI Inc. • Effective Date: May 12, 2026 • Last Updated: May 12, 2026

---

1. Introduction and Scope

1.1. This Data Processing Agreement ("DPA") forms part of, and is incorporated into, the Merchant Services Agreement or other applicable service agreement ("Agreement") between **InsightPlay AI Inc.**, a Delaware corporation ("Processor," "InsightPlay," "we," or "us"), and the entity identified in the Agreement ("Controller," "Client," "you," or "your").

1.2. This DPA sets out the terms, requirements, and conditions on which InsightPlay will process Personal Data on behalf of the Client in connection with the provision of InsightPlay's AI-powered platform and related services (the "Services").

1.3. This DPA applies to the extent that InsightPlay processes Personal Data that is subject to applicable Data Protection Laws on behalf of the Client. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

1.4. The parties agree that the Client is the **Data Controller** and InsightPlay is the **Data Processor** in respect of Personal Data processed under this DPA, unless otherwise specified.

2. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Any capitalized terms not defined herein shall have the meanings assigned to them in the Agreement.

"Data Protection Laws" means all applicable laws and regulations relating to the processing, privacy, and security of Personal Data, including but not limited to: (a) the General Data Protection Regulation (EU) 2016/679 ("GDPR"); (b) the UK General Data Protection Regulation and Data Protection Act 2018 ("UK GDPR"); (c) the Colombian Law 1581 of 2012 and Decree 1377 of 2013; (d) the Argentine Personal Data Protection Law No. 25,326; (e) the Mexican Federal Law on Protection of Personal Data Held by Private Parties; (f) the Panama Law 81 of 2019; and (g) any other applicable data protection or privacy legislation in the jurisdictions in which the Services are provided.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates, including end users, players, or customers of the Client.

"Personal Data" means any information relating to a Data Subject that is processed by InsightPlay on behalf of the Client in connection with the Services, as further described in Annex 1.

"Personal Data Breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

"Processing" (and its derivatives "Process," "Processed") means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

"Sub-processor" means any third party engaged by InsightPlay to Process Personal Data on behalf of the Client.

"Supervisory Authority" means any regulatory body or authority with jurisdiction over data protection matters in the relevant jurisdiction.

"Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses for the transfer of personal data to processors established in third countries, as adopted by the European Commission or other competent authority, as applicable.

3. Processing of Personal Data

3.1. **Instructions.** InsightPlay shall Process Personal Data only on documented instructions from the Client, including with respect to transfers of Personal Data to a third country, unless required to do so by applicable law, in which case InsightPlay shall inform the Client of that legal requirement before Processing (unless the law prohibits such notification on important grounds of public interest).

3.2. **Purpose Limitation.** InsightPlay shall Process Personal Data solely for the purpose of providing the Services as described in the Agreement and this DPA. InsightPlay shall not Process Personal Data for any other purpose, including for its own purposes, unless explicitly authorized in writing by the Client.

3.3. **Details of Processing.** The subject matter, duration, nature, and purpose of Processing, the types of Personal Data, and the categories of Data Subjects are described in **Annex 1** of this DPA.

3.4. **Compliance.** Each party shall comply with its obligations under applicable Data Protection Laws. The Client shall ensure that its instructions to InsightPlay are lawful and that it has obtained all necessary consents, authorizations, and legal bases for the Processing of Personal Data by InsightPlay.

3.5. **AI-Specific Processing.** The Client acknowledges that the Services involve AI-driven processing of Personal Data, including natural language processing, voice analysis, dialogue management, and automated decision-making in connection with player communications. InsightPlay shall:

- Process voice recordings and transcripts solely for delivering and improving the contracted Services;
- Not use Personal Data to train general-purpose AI models outside the scope of the Client's Services without explicit written consent;
- Ensure that AI-generated outputs (e.g., call transcripts, campaign analytics) are accessible to the Client and treated as Client data; and
- Support the Client in fulfilling Data Subject rights related to automated decision-making, including the right to obtain human intervention where required by applicable law.

4. Obligations of the Processor

4.1. **Confidentiality.** InsightPlay shall ensure that all personnel authorized to Process Personal Data have committed to confidentiality obligations, whether by contract or statutory duty, and are aware of and comply with this DPA.

4.2. **Security Measures.** InsightPlay shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful Processing, accidental loss, destruction, or damage, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk to Data Subjects. Such measures are described in **Annex 2** and shall include, at a minimum:

- Encryption of Personal Data in transit and at rest;
- Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems;
- Access controls and authentication mechanisms;
- Regular testing, assessing, and evaluating the effectiveness of security measures;
- Incident detection and response capabilities; and
- Secure disposal of Personal Data upon termination or request.

4.3. **Assistance.** Taking into account the nature of Processing, InsightPlay shall assist the Client, by appropriate technical and organizational measures and insofar as is reasonably possible, in fulfilling the Client's obligations to respond to Data Subject requests exercising their rights under applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection).

4.4. **Cooperation.** InsightPlay shall assist the Client in ensuring compliance with its obligations regarding security of Processing, notification of Personal Data Breaches, data protection impact assessments, and prior consultations with Supervisory Authorities, taking into account the nature of Processing and the information available to InsightPlay.

4.5. **Records.** InsightPlay shall maintain records of Processing activities carried out on behalf of the Client in accordance with applicable Data Protection Laws and shall make such records available to the Client upon request.

5. Sub-processing

5.1. **General Authorization.** The Client provides InsightPlay with general written authorization to engage Sub-processors for the Processing of Personal Data in connection with the Services. InsightPlay shall maintain a current list of Sub-processors, which shall be made available to the Client upon request or published at www.insightplay.ai/sub-processors.

5.2. **Notification of Changes.** InsightPlay shall notify the Client of any intended changes to the list of Sub-processors (additions or replacements) at least fifteen (15) days prior to engaging the new Sub-processor. The Client may reasonably object to the appointment of a new Sub-processor by notifying InsightPlay in writing within ten (10) days of receiving such notice. If the Client objects, the parties shall discuss the concern in good faith. If no resolution is reached, the Client may terminate the affected Services without penalty upon thirty (30) days' written notice.

5.3. **Sub-processor Obligations.** InsightPlay shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set out in this DPA. InsightPlay shall remain fully liable to the Client for the performance of each Sub-processor's obligations.

5.4. **Current Sub-processors.** The categories of Sub-processors engaged by InsightPlay as of the effective date of this DPA are described in **Annex 3**.

6. International Data Transfers

6.1. InsightPlay shall not transfer Personal Data to a country or territory outside the jurisdiction in which it was collected unless appropriate safeguards are in place in accordance with applicable Data Protection Laws.

6.2. Where Personal Data originating in the European Economic Area (EEA), the United Kingdom, or Switzerland is transferred to a country not recognized as providing an adequate level of data protection, InsightPlay shall ensure that such transfers are made subject to the Standard Contractual Clauses or other approved transfer mechanisms under applicable law.

6.3. Where Personal Data originating in Colombia, Argentina, Mexico, Panama, or other Latin American jurisdictions is transferred internationally, InsightPlay shall comply with the applicable cross-border data transfer requirements, including obtaining necessary authorizations from the relevant Supervisory Authorities where required.

6.4. InsightPlay shall inform the Client of the countries in which Personal Data is Processed and stored, and shall update the Client of any changes.

7. Personal Data Breach Notification

7.1. InsightPlay shall notify the Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of the Client.

7.2. Such notification shall include, to the extent available:

- A description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records affected;

- The name and contact details of InsightPlay's designated contact for further information;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

7.3. InsightPlay shall cooperate with the Client and take reasonable steps to assist in the investigation, mitigation, and remediation of the Personal Data Breach.

7.4. InsightPlay's notification of a Personal Data Breach shall not be construed as an acknowledgment of fault or liability.

8. Data Subject Rights

8.1. InsightPlay shall promptly notify the Client if it receives a request from a Data Subject to exercise their rights under applicable Data Protection Laws (including access, rectification, erasure, restriction, portability, objection, or rights related to automated decision-making).

8.2. InsightPlay shall not respond to such requests directly unless authorized by the Client or required by applicable law, in which case InsightPlay shall inform the Client prior to responding (unless prohibited by law).

8.3. InsightPlay shall provide the Client with reasonable technical and organizational assistance to enable the Client to fulfill Data Subject requests, including by providing tools or functionality within the platform to access, export, correct, or delete Personal Data.

9. Audits and Inspections

9.1. InsightPlay shall make available to the Client all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA.

9.2. InsightPlay shall allow for and contribute to audits, including inspections, conducted by the Client or an independent third-party auditor mandated by the Client, subject to the following conditions:

- The Client shall provide at least thirty (30) days' prior written notice of any audit;
- Audits shall be conducted during normal business hours, no more than once per twelve (12) month period (unless required by a Supervisory Authority or in response to a Personal Data Breach);
- The auditor shall be bound by confidentiality obligations; and
- The audit shall be conducted in a manner that minimizes disruption to InsightPlay's operations.

9.3. Where InsightPlay has obtained relevant third-party certifications or audit reports (e.g., SOC 2 Type II, ISO 27001), it may provide these to the Client as evidence of compliance in lieu of a physical audit, at InsightPlay's discretion.

10. Data Retention and Deletion

10.1. Upon termination or expiration of the Agreement, or upon the Client's written request, InsightPlay shall, at the Client's election, return all Personal Data to the Client in a commonly used, machine-readable format, or securely delete or destroy all Personal Data in its possession, including all copies, within thirty (30) days.

10.2. InsightPlay shall provide written confirmation of deletion or destruction upon the Client's request.

10.3. InsightPlay may retain Personal Data to the extent required by applicable law, provided that such retained data remains subject to the confidentiality and security obligations of this DPA. InsightPlay shall inform the Client of any such legal retention requirement.

10.4. Obligations regarding data retention and deletion extend to all Sub-processors engaged by InsightPlay.

11. Liability

11.1. Each party's liability arising out of or related to this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement, except to the extent that applicable Data Protection Laws prohibit such limitations.

11.2. For the avoidance of doubt, nothing in this DPA limits either party's liability for: (a) Personal Data Breaches caused by willful misconduct or gross negligence; (b) fines or penalties imposed directly on that party by a Supervisory Authority; or (c) any liability that cannot be limited under applicable law.

12. Term and Termination

12.1. This DPA shall remain in effect for as long as InsightPlay Processes Personal Data on behalf of the Client.

12.2. The obligations of InsightPlay under this DPA with respect to the security and confidentiality of Personal Data shall survive the termination or expiration of this DPA and the Agreement until all Personal Data has been returned or securely destroyed.

13. General

13.1. **Governing Law.** This DPA shall be governed by the laws of the State of Delaware, United States of America, without prejudice to mandatory data protection provisions of the jurisdiction(s) in which Personal Data is collected or in which Data Subjects are located.

13.2. **Amendments.** InsightPlay may update this DPA to reflect changes in Data Protection Laws or Processing activities. Material changes will be communicated to Clients with reasonable notice.

13.3. **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

13.4. **Contact.** For questions or requests regarding this DPA, please contact:

InsightPlay AI Inc. • Data Protection Contact: privacy@insightplay.ai • Website: www.insightplay.ai

Annex 1: Details of Processing

Element	Description
Subject matter	Processing of Personal Data in connection with AI-powered voice and text communication services for iGaming operators.
Duration	For the term of the Agreement plus any period required for data return or deletion.
Nature of Processing	Collection, storage, organization, retrieval, use, transmission, recording, transcription, analysis, and deletion of Personal Data through automated AI-driven systems.
Purpose of Processing	Player acquisition, reactivation, and retention campaigns; inbound and outbound AI voice and text communications; customer support automation; campaign performance analytics and reporting; platform configuration and AI agent training.
Types of Personal Data	Name; telephone number(s); email address; player/user ID; account status and activity history; call recordings and transcriptions; communication preferences; campaign interaction data; IP address and device identifiers (where applicable); geolocation data (country/region level); any additional data provided by the Client for

	campaign configuration.
Categories of Data Subjects	End users, players, and customers of the Client; prospective players targeted through acquisition campaigns; inactive players targeted through reactivation campaigns.
Special categories of data	None intended. The Client shall not provide special category data unless explicitly agreed in writing.

Annex 2: Technical and Organizational Security Measures

InsightPlay implements and maintains the following categories of security measures. Specific controls may be updated from time to time to reflect evolving best practices and regulatory requirements.

1. Access Control

- Role-based access controls (RBAC) with principle of least privilege
- Multi-factor authentication (MFA) for all platform and infrastructure access
- Unique user credentials; no shared accounts
- Regular access reviews and prompt deprovisioning upon personnel changes

2. Encryption

- Encryption of Personal Data in transit using TLS 1.2 or higher
- Encryption of Personal Data at rest using AES-256 or equivalent
- Secure key management practices

3. Network and Infrastructure Security

- Firewalls, intrusion detection and prevention systems
- Network segmentation and monitoring
- Regular vulnerability scanning and penetration testing
- Secure cloud infrastructure with reputable providers (e.g., GCP, AWS)

4. Application Security

- Secure software development lifecycle (SDLC) practices
- Code reviews and security testing prior to deployment
- Regular patching and updates

5. Data Handling

- Data minimization principles applied to Processing activities
- Logical separation of Client data
- Secure deletion and destruction procedures

6. Personnel

- Confidentiality agreements for all personnel with access to Personal Data
- Security awareness training upon onboarding and periodically thereafter
- Background checks where permitted by law

7. Incident Response

- Documented incident response plan
- Designated incident response team
- Regular testing and review of incident response procedures

8. Business Continuity

- Regular backups with tested restoration procedures
- Disaster recovery planning

- Redundant infrastructure and failover capabilities

9. Physical Security

- Data center access controls (managed by cloud infrastructure providers)
- Environmental controls for on-premise equipment (where applicable)

Annex 3: Sub-processors

InsightPlay engages the following categories of Sub-processors. A current, named list is available upon request or at www.insightplay.ai/sub-processors.

Category	Purpose	Location(s)
Cloud infrastructure provider(s)	Hosting, storage, and compute for the InsightPlay platform	United States
Telephony and voice provider(s)	Outbound and inbound call routing, SIP trunking, voicemail detection	United States, regional
AI model and speech processing provider(s)	Natural language processing, speech-to-text, text-to-speech	United States
Messaging platform provider(s)	WhatsApp, SMS, and other text-based communication channels	United States, regional
Analytics and monitoring provider(s)	Platform performance monitoring, logging, and operational analytics	United States
Customer support tooling provider(s)	Ticketing and support workflow management	United States

The Client will be notified of changes to Sub-processors in accordance with Section 5.2 of this DPA.

This Data Processing Agreement is provided as part of InsightPlay AI Inc.'s Trust Center. The specific data processing terms governing any client engagement are defined in the applicable Merchant Services Agreement and its schedules.