OBIANSWERS | CUSTOMER DATA PROTECTION ADDENDUM

Data Processing Agreement

OBIAnswers

Version: 2026-10-28.1 | **Issued:** October 28, 2026

This Data Processing Agreement ("DPA") is between **ARGMEDIAGROUP LLC** ("Company") and the business customer identified in the applicable accepted OBIAnswers Order and workspace registration records ("Customer"). It supplements their OBIAnswers SaaS License & Subscription Agreement and applicable Order (together, the "Agreement") for personal information Company processes on Customer's behalf.

Customer accepts this DPA through an explicit electronic acceptance process identifying this DPA, or through a mutually accepted written Order or amendment expressly incorporating it. Company offers this DPA and becomes bound when Customer validly accepts it. An authorized adult must accept for Customer. A separate handwritten signature is not required; an ordinary employee login does not constitute acceptance for Customer.

1. Scope, roles and precedence

1.1 Definitions. "Customer Personal Data" means personal information contained in Customer Content and related workspace records that Company processes on Customer's behalf. "Data Protection Law" means privacy and data-protection laws applicable to that processing, including GDPR, UK GDPR and applicable U.S. state privacy laws to the extent each applies. "Subprocessor" means a provider engaged by Company to process Customer Personal Data for Customer. "Personal Data Breach" means a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. Other capitalized terms have the meaning given in the Agreement.

1.2 Roles. Customer acts as controller or equivalent business, and Company as processor, service provider or contractor for the covered processing. If Customer itself acts as processor, it must have authority from its controller to appoint Company, communicate binding lawful instructions and permit the processing and Subprocessors. Company does not acquire a right to determine unrelated purposes for Customer Personal Data. Actual responsibilities under applicable law prevail over labels.

1.3 Other information. Company independently administers its own business-contact, payment, compliance and proportionate security records as described in the Privacy Policy. That distinction does not authorize Company to repurpose Customer's documents, questions, answers or employee records for unrelated uses. A provider may have a separate role for payment, fraud, or legal obligations; that processing is not automatically Subprocessor activity under this DPA.

1.4 Priority and duration. This DPA controls conflicts concerning its personal-data processing subject matter. Mandatory transfer terms and Data Protection Law control to the extent required. The remaining Agreement, including commercial terms, remains in effect. This DPA continues while Company or its Subprocessors retain Customer Personal Data, including permitted wind-down or legally required retention. Annexes A-C form part of this DPA. This DPA does not itself change subscription pricing, payment deadlines or purchasing authority.

01 | OBLIGATIONS OF CUSTOMER AND COMPANY

Instructions, purpose & restricted uses

2. Customer instructions and responsibilities

2.1 Documented instructions. The Agreement, this DPA, accepted Orders, lawful use of configuration and access controls, and verified written directions from authorized Customer representatives constitute Customer's documented instructions. Company will process Customer Personal Data only for the purposes and activities in Annex A and those instructions, including instructions for transfers, unless applicable law requires otherwise. Company will notify Customer before legally required processing unless prohibited on lawful public-interest grounds.

2.2 Unlawful or additional instructions. Company will promptly inform Customer if it considers an instruction to infringe applicable data-protection requirements. Company may pause the affected instruction while the parties resolve it and must not follow a known unlawful instruction. Customer may not require unsupported processing or expanded purposes without mutual written agreement and necessary safeguards. A dispute about optional services does not excuse mandatory assistance or protection duties.

2.3 Customer duties. Customer must establish lawful grounds, provide required notices, obtain required permissions, ensure accuracy and necessity of submissions, assign appropriate roles and document audiences, and respond to individuals in its controller role. It must not submit restricted data without the required approval. Customer must maintain authoritative originals and independent business continuity arrangements. Company remains responsible for its own obligations notwithstanding Customer's duties.

2.4 Younger employees and sensitive data. This DPA does not authorize under-13 accounts, waive higher local age requirements, or replace a required minor-access addendum, age assurance or parental authorization. Eligible younger-employee processing requires compliance with the Terms and an expressly approved arrangement resolving any children's-data restriction in the Agreement. Special-category data, criminal-offence data, protected health information, payment authentication data and other restricted information may not be intentionally submitted unless specifically approved in a written addendum establishing lawful processing and safeguards.

3. Company duties and processing restrictions

3.1 Purpose limitation. Company will collect, retain, use and disclose Customer Personal Data only to perform the limited service purposes in Annex A, follow lawful instructions, or meet an applicable legal requirement. It will not sell the data; share it for cross-context behavioral advertising; use it for unrelated advertising; or use or permit its use to train general-purpose AI models without separate express authorization and any additional legally required grounds. Service generation and retrieval are not permission for unrelated model training.

3.2 Confidentiality and access. Company will ensure persons authorized to process Customer Personal Data are bound to appropriate contractual or statutory confidentiality duties, receive appropriate security and privacy guidance for their role, and have access limited to operational need. Company will maintain safeguards described in Annex B, taking account of processing risks, available technology, implementation cost and applicable law. It may improve controls without materially reducing protection.

3.3 U.S. service-provider terms. Where applicable U.S. state law treats Company as a service provider or contractor, Company will provide the required level of privacy protection, comply with applicable duties, and not retain, use or disclose data outside the direct business relationship or for a commercial purpose unrelated to Annex A, except where expressly permitted by that law. It will not combine the data with information from other customers, independent consumer interactions or other sources except where legally permitted for the specified service purposes. Company certifies that it understands and will comply with these restrictions.

3.4 Inability to comply. Company will promptly notify Customer if it can no longer meet applicable processing obligations and cooperate on reasonable steps to stop and remediate unauthorized use. Customer may take reasonable and appropriate steps to verify processing and require correction within the audit and assistance framework below. These rights do not permit access to another customer's information.

02 | DELEGATED PROCESSING AND INTERNATIONAL SAFEGUARDS

Providers, transfers & incidents

4. Subprocessors

4.1 Authorization and register. Customer gives general written authorization for Subprocessors disclosed in the applicable register under Annex C, subject to this section. Before a Subprocessor processes covered data, Company must disclose its legal identity, relevant function and processing locations in a register available to Customer, ensure appropriate diligence, and enter written terms imposing equivalent applicable data-protection obligations. Company remains responsible for a Subprocessor's performance of its delegated duties to the extent required by law and this DPA.

4.2 Changes and objections. Company will give at least 30 calendar days' advance notice of a new or replacement Subprocessor before it receives Customer Personal Data, unless a shorter period is necessary for an urgent security or legal reason and lawful; in that case it will notify Customer promptly and minimize affected processing. Customer may object on reasonable, documented data-protection grounds within 15 days after notice, or a longer legally required period. The parties will seek a reasonable alternative or mitigation. A mandatory local objection right is not shortened by this period.

4.3 Unresolved objection. If the parties cannot resolve a timely, substantiated objection before the affected processing begins, Company must avoid that processing for Customer or Customer may terminate the affected service without penalty. Company will refund unused prepaid fees for that terminated portion and unused associated purchased credits. Additional assistance or data export remains governed by the Agreement and law. An emergency change is not permission to bypass required transfer safeguards.

5. International transfers

5.1 Transfer conditions. Customer authorizes processing in disclosed locations only where allowed by its instructions and Data Protection Law. Company will identify relevant locations and onward recipients on request and assist Customer with required transfer assessments using reasonably available information. No particular residency commitment or privacy-framework certification is created by this DPA. Ordinary consent to use the Service is not blanket consent to a restricted international transfer.

5.2 Required instruments. Before a transfer requiring additional safeguards, the parties must establish a valid transfer mechanism, such as an applicable adequacy decision or completed approved contractual safeguards, and any required supplementary measures. Where EU Standard Contractual Clauses, a UK Addendum or IDTA, or other local clauses are required, the applicable instrument, parties, roles, module, annexes, competent authority, governing law and other required selections must be completed and validly agreed. This DPA does not automatically execute or substitute for those instruments. Until the required mechanism is established, the affected transfer must not proceed. Mandatory transfer terms take precedence over inconsistent dispute or liability terms.

6. Personal Data Breaches

6.1 Notification and cooperation. Company will notify Customer without undue delay after becoming aware of a Personal Data Breach and within any shorter applicable mandatory deadline. Notification will not be delayed until every fact is known or final attribution is complete. It will provide information then available concerning the nature of the breach, affected data and individuals, likely consequences, mitigation and a contact point, and provide reasonable updates as investigation proceeds.

6.2 Response. Company will take reasonable containment, remediation and evidence-preservation steps and cooperate with Customer's lawful assessment and notification duties. Customer generally determines notifications to individuals or regulators for its controlled data; Company may notify where law directly requires it and will coordinate where permitted. Notification is not an admission of liability. Unsuccessful attempts that do not compromise covered data are not, by themselves, Personal Data Breaches, but may be addressed through security operations.

03 | ACCOUNTABILITY AND ASSISTANCE

Requests, audits & service termination

7. Assistance and verification

7.1 Individual requests. Company will promptly inform Customer of a request concerning Customer-controlled data where permitted and reasonably assist Customer to meet lawful response deadlines through available access, correction, export, restriction or deletion functions and support. Company will not independently determine Customer's response unless authorized or legally required. Identity verification must be proportionate. Company will respond directly to requests concerning processing for which it is independently responsible, without using role allocation to defeat individual rights.

7.2 Risk assessments and authorities. Taking account of the nature of processing and information available, Company will reasonably assist Customer with data-protection impact assessments, prior consultations, processing records, regulator inquiries and applicable security, breach and other controller obligations. Company will maintain records and cooperate with competent supervisory authorities as required. Lawful compelled disclosures will be limited appropriately, with advance notice where permitted.

7.3 Evidence and audits. Company will make information reasonably necessary to demonstrate compliance available and allow and contribute to audits, including inspections, by Customer or an independent auditor it appoints. Review will ordinarily begin with available documentation. Inspections must use reasonable notice, scope, confidentiality and security precautions and avoid unnecessary disruption or exposure of others' data. Routine customer-initiated inspections ordinarily occur no more than once yearly, but that limit does not apply to a regulator requirement, a substantiated material concern, a relevant breach, or a legally required audit. A nonexistent certificate cannot substitute for evidence.

7.4 Assistance costs. The parties may agree reasonable advance fees for extraordinary assistance beyond ordinary Service functions. No charge or procedural condition may obstruct a mandatory right or deadline. Company bears assistance costs attributable to its material breach of this DPA. Customer bears its independent auditor costs unless otherwise required by law or mutually agreed. Each party must cooperate reasonably on scope and timing.

8. Return, deletion and retention

8.1 Customer choice. At the end of the processing services, Company will, at Customer's choice and lawful direction, return or delete Customer Personal Data and delete remaining copies unless law requires retention. The Agreement's standard 30-day retrieval window permits an orderly export; it does not postpone an earlier lawful deletion instruction or a mandatory deadline. Company will supply routine available exports or reasonable support-assisted retrieval after appropriate verification. Company may charge only agreed fees for bespoke conversion or migration.

8.2 Standard wind-down. Absent an earlier lawful instruction or overriding requirement, Company will delete or de-identify active Customer Content within 60 days after the 30-day retrieval period ends and expire residual backups no later than 180 days after termination, consistent with the Agreement. If applicable law requires an earlier outcome or deletion of all copies, that duty controls. Company will direct relevant Subprocessors to perform required deletion and provide reasonable confirmation on request.

8.3 Protected residual copies. Information retained because of binding law or a valid legal hold must be limited to that purpose and protected. Residual backups must not be used for ordinary product operations and must be isolated from routine access. If a backup is restored, applicable deletion and access restrictions must be reapplied. Irreversible de-identification must satisfy the applicable legal standard; merely removing a visible name is not necessarily sufficient.

9. Liability, disputes and contact

The Agreement's liability allocation and dispute provisions apply to the extent lawful; this DPA creates no additional monetary cap or separate automatic indemnity. No contractual limit restricts a regulator's powers, an individual's non-waivable rights, or mandatory transfer-clause remedies. Data-protection obligations continue while covered data is retained and are not erased by a payment dispute. Amendments require valid mutual acceptance, subject to lawful Subprocessor changes under Section 4. Notices follow the Agreement; privacy and security correspondence may be sent to contact@argmediagroup.com. Company's address is 111 Town Square Pl, Ste 1238, PMB 659533, Jersey City, New Jersey 07310-1810, United States.

ANNEX A AND ANNEX B | PART OF THIS DPA

Processing description & security measures

Annex A - Description of covered processing

A.1 Subject matter and nature. Provision of the OBIAnswers business knowledge service: collection and receipt; storage and organization; extraction, indexing and retrieval of uploaded content; AI generation; display and sharing within authorized workspace audiences; question and review history; access administration; authorized exports; troubleshooting and security; and return or deletion. Customer's verified configuration and approved instructions define the workspace and audience.

A.2 Specific service purposes. Enable authorized employees to locate guidance in Customer-approved materials; obtain source-referenced answers; request manager clarification; curate approved answers; administer membership and document audiences; maintain usage and operational audit records; resolve service errors; and deliver requested account or review-related communications. These purposes do not include unrelated advertising, general-purpose model training or commercial sale of personal information.

A.3 Individuals and categories. Individuals may include Customer's employees, invited contractors, managers, administrators, business contacts and persons whose information Customer lawfully includes in approved documents or questions. Categories may include names, work contact information, usernames, role and membership identifiers, work location or department assignments, access and verification status, submitted document content and metadata, questions and answers, citations, feedback and review context, timestamps, usage and diagnostic identifiers, and communication records. Payment-card credentials are not part of the instructed workspace processing.

A.4 Frequency and duration. Processing is ongoing and event-driven during Customer's subscription, including document uploads, user requests and support, followed by the authorized retrieval and deletion period. Customer determines the ordinary volume and content within purchased limits. Retention follows Section 8 and applicable instructions. Restricted data, minor-user eligibility and required approvals are governed by Section 2.4; their inclusion in Customer submissions does not automatically authorize them.

Annex B - Technical and organizational measures

Company will maintain measures appropriate to the risks of covered processing. The following describe the baseline commitments; they are not a promise of a named audit certification, fixed backup frequency, guaranteed uptime or zero risk.

B.1 Access control and separation. Authenticate users through managed identity services; protect sessions; verify current workspace membership, role and status at the server; apply document-audience restrictions; and separate customer data through organization-scoped storage, records and retrieval filters. Administrative access must be restricted to authorized personnel and reviewed when duties change.

B.2 Transport, credentials and source access. Use encrypted network connections for supported service and provider communications; restrict server-side credentials from client code; protect database and object storage through access rules and provider controls; and authorize source viewing with short-lived links or equivalent controls. Customer must protect its own devices, user assignments and credentials.

B.3 Ingestion and AI controls. Validate supported upload types and size limits, constrain processing jobs, use organization and authorized-document retrieval filters, and verify source access before returning references. Treat uploaded material as untrusted input. These safeguards reduce unauthorized access risk but do not guarantee every AI answer is accurate or every malicious instruction will be detected.

B.4 Operational safeguards. Maintain appropriate event and error records, avoid intentionally logging full documents or credentials, restrict logs, manage vulnerabilities and updates, investigate incidents, and maintain proportionate recovery and secure-deletion procedures. Maintain confidentiality obligations and staff guidance. Use managed-provider protection and monitor service health. Make relevant evidence available under Section 7; do not claim a control was independently certified unless supported.

ANNEX C | PART OF THIS DPA

Provider register & acceptance

Annex C - Subprocessor functions and disclosure

The following provider groups describe the Service's processing architecture. A provider is a Subprocessor under this DPA only for activities in which it processes Customer Personal Data on Company's behalf. A register supplied to Customer before the relevant processing must identify the contracted legal entity, the relevant locations and functions, and any necessary transfer safeguard. Group names alone do not establish a particular residency location or executed transfer instrument.

C.1 Google/Firebase and Google Cloud. Managed account identity, workspace database and object storage, document processing infrastructure and task execution, and relevant app-attestation or security functions. Covered information may include account and membership data, documents and extracted text, stored questions and answers, reviews and operational records, to the extent used for Customer's service.

C.2 OpenAI. Document file storage and indexing, retrieval of authorized sources, answer generation and related safety functions. Covered information may include document text, questions, relevant retrieved material, business instructions and user-related safety identifiers. Files and search indexes may remain until deleted; no zero-retention promise is created. The no-general-purpose-training restriction in Section 3 applies independently of operational retention.

C.3 Vercel. Website hosting and delivery, processing of application requests, operational logging and relevant performance functions where enabled. Covered information may include request and device metadata and information necessarily handled in delivering Customer's application sessions. Independently controlled aggregate website measurements, where outside instructed workspace processing, are described in the Privacy Policy and remain subject to law.

C.4 Resend. Delivery of transactional account, invitation, security, review or support communications where the feature is used and configured. Covered information is limited to necessary recipient/contact information, message content and delivery metadata. Full workspace documents are not included merely because a notification is delivered; any additional disclosure requires lawful instructions.

C.5 Payment and independent services. Stripe provides hosted payments and billing. Where it handles payment or fraud information as an independent controller, it is not a Subprocessor merely because it is listed in the Privacy Policy. Any activity that actually processes covered data as a Subprocessor must instead satisfy this DPA. Customer's independently selected integrations and its own recipients remain subject to the appropriate separate arrangements; Company's obligations cannot be avoided by mislabeling its own processing providers.

Acceptance and processing records

The Customer legal entity, business contact, workspace identifier and authorized representative are identified in its accepted Order and relevant account records. Customer's designated business contact is the DPA contact unless Customer gives a replacement in writing. Company's DPA contact is contact@argmediagroup.com. Before processing that requires it, Customer must identify its controller or processor role and communicate relevant location, transfer and restricted-data requirements.

Company will retain evidence of Customer's affirmative acceptance, the accepted DPA version, the incorporated Order, acceptance date and representative account, and the applicable Subprocessor register. Customer will have a reasonable opportunity to download and retain the DPA. Company must obtain valid acceptance of a material amendment; a passive website visit or ordinary employee account login is not a substitute for authorized business acceptance.

This DPA supplies the general customer-processing terms. Required local or international-transfer instruments and any minor-access or regulated-data addendum must be separately completed and accepted before the affected activity. It does not establish a global compliance certification or authorize processing that applicable law prohibits.

End of Data Processing Agreement. Sections 1-9 and Annexes A-C form the complete DPA, subject to expressly accepted additional instruments and the precedence rules above.