OBIANSWERS | ARGMEDIAGROUP LLC

Privacy Policy

OBIAnswers

Last updated: October 28, 2026 | **Version:** 2026-10-28.1

This Privacy Policy explains how **ARGMEDIAGROUP LLC** ("OBIAnswers," "we," "us," or "our") collects, uses, discloses, and retains personal information in connection with the OBIAnswers website, hosted business knowledge platform, supported mobile applications, account administration, and related communications (the "Service").

OBIAnswers helps businesses organize their documents and provide authorized employees with AI-assisted answers, source references, approved knowledge, and manager-review workflows. Information submitted to a business workspace may be visible to authorized managers and administrators. Do not treat workplace questions or uploaded documents as private from your organization.

1. Who is responsible for your information

Information we manage for our own purposes. We determine how and why account administration, billing contacts, inquiries, security, fraud prevention, website operations, and legal-compliance information are processed. Where applicable, we act as a controller or equivalent business responsible for those purposes.

Information processed for a business customer. For personal information in customer documents, workspace questions, answers, reviews, and related business records, the customer generally determines the purposes and instructions and we provide processing services on its behalf. The customer's agreement, any applicable data processing addendum (DPA), its own notices, and applicable law govern those activities. A contractual label does not override the parties' actual legal responsibilities.

Employee and invited-user requests. Your employer or other workspace organization may be the appropriate first contact for access to, correction of, or deletion of its business records. You may also contact us; we will identify our role and assist or route the request as appropriate. We do not require you to waive individual privacy rights because information appears in a business workspace.

2. How to contact us

Privacy contact: contact@argmediagroup.com
Postal address: ARGMEDIAGROUP LLC
111 Town Square Pl, Ste 1238, PMB 659533
Jersey City, New Jersey 07310-1810, United States

Please identify the account or workspace involved and the nature of your request. Do not send passwords, full payment-card details, or unnecessary sensitive information. We may request proportionate information to verify identity or authority before disclosing, changing, exporting, or deleting records.

This Policy is a privacy notice, not blanket consent to processing, an automatic enrollment in marketing, or a waiver of legal rights. Separate consent or authorization will be used where required.

01 | CATEGORIES AND SOURCES

Information we collect

3. Information you and your organization provide

Account and professional information. Name, username, email address, job title, phone number where provided, contact preference, account identifiers, authentication and email-verification status, and account settings. Passwords and sign-in credentials are handled through our authentication services; do not include them in documents or support messages.

Organization and access information. Company name, business profile, website, business location and address details where provided, workspace identifiers, membership, role, status, department or location assignments, invitations, and administrative actions. Workplace location information is distinct from precise device GPS location.

Documents and derived knowledge. Uploaded documents and their contents, file metadata, extracted text, document-access rules, processing and indexing status, source mappings, approved answers, versions, and archive or deletion actions. These records may include information about employees, customers, or other individuals if your organization supplies it.

Questions, answers and reviews. Questions, generated answers, source references, answer status, saved history, feedback, manager-review requests, follow-up context, and manager responses. We store business interaction history so authorized users can revisit answers and manage knowledge.

Billing and referrals. Billing contact and address, selected plan, subscription and invoice status, payment-provider customer and transaction identifiers, purchase amounts, tax information where required, referral codes, attribution, qualifying subscription events, and discount progress. Stripe-hosted payment pages collect payment-method details; our hosted checkout integration does not give us full payment-card numbers.

Communications and preferences. Support requests, error reports you submit, correspondence, requested follow-up details, and available privacy, AI-processing, or communication preferences. Information you voluntarily email is processed to address your message.

4. Information collected through use

We and our infrastructure providers process technical and usage information such as IP address, browser or device characteristics, operating system, requested pages and endpoints, timestamps, session and security identifiers, referral information, page-view and performance events, error categories, usage counts, and operational or audit activity. Approximate location may be derived from an IP address. Security tools may use app-attestation or device-integrity signals to detect unauthorized requests.

Information comes directly from you, your organization and its administrators, your use of the Service, and providers that supply authentication, payment, email-delivery, hosting, and technical status information. We do not need unrelated sensitive personal information for ordinary use. Do not upload restricted information identified in the Terms or customer agreement.

02 | HOW INFORMATION IS USED AND DISCLOSED

Purposes, AI & service providers

5. Why we process information

We use relevant information to create and authenticate accounts; verify email; deliver invitations and account messages; enforce workspace permissions; process and index documents; retrieve authorized knowledge; generate and store answers; support manager review; administer subscriptions, credits and referrals; provide exports and account controls; respond to support and privacy requests; monitor usage and performance; detect abuse and fraud; investigate errors; secure the Service; and comply with legal duties or resolve disputes.

Where law requires a legal basis for processing we control, we rely on contract performance when dealing directly with an individual contracting party; legitimate interests in operating, supporting and securing a business service where those interests are not overridden by individual rights; legal obligations; and consent where required. Employee data processing does not automatically rely on the employer's contract as the employee's own contractual legal basis. Customer-controlled workspace processing follows the customer's lawful instructions and appropriate legal grounds. You may ask us which basis applies to a particular activity.

6. AI processing and model training

To provide AI features, we send uploaded documents or extracted content to OpenAI for indexing and retrieval, and send questions, relevant source material, applicable business instructions, and a user-related safety identifier for answer generation and abuse prevention. The identifier is not necessarily anonymous. We also save questions, answers and references in the workspace. Authorized content and permissions determine what the application makes available to users.

We do not use customer documents, questions or answers to train general-purpose AI models or authorize providers to do so without separate express permission. OpenAI states that API inputs and outputs are not used for model training by default. This is different from data retention: document files and search indexes may remain until deleted, and providers may retain security, abuse-monitoring or operational records under their applicable service terms. OBIAnswers does not promise zero retention. Available AI controls affect future feature use; withdrawing consent does not automatically erase previously stored workspace or provider records.

7. Providers and other recipients

We disclose information necessary for the following service functions. Providers may act as processors, service providers or independent controllers for particular activities, according to their role and applicable terms:

Google/Firebase and Google Cloud. Authentication, database and file storage, processing infrastructure, task delivery, and app-integrity or security services.

OpenAI. AI document storage, indexing, retrieval, answer generation, and relevant safety or abuse-prevention processing.

Stripe. Hosted payments, subscription administration, invoices, billing management, tax-related checkout functions, and payment-security activities.

Vercel. Website hosting and delivery, operational logs, and web analytics or performance monitoring where enabled.

Resend. Delivery of account, invitation, security, transactional or support-related emails, including necessary recipient and message information.

We may also disclose necessary information to authorized personnel, contractors and professional advisers for support, security, legal or administrative purposes; to authorities when legally required; and to a buyer or successor in a proposed or completed business transaction subject to appropriate confidentiality and applicable privacy obligations. We may disclose information with your valid direction or authorization. Contact us for information about relevant processing providers and safeguards.

03 | SHARING, CONTROLS AND INTERNATIONAL PROCESSING

Workspace access, cookies & transfers

8. Workspace visibility and permitted sharing

Owners, administrators and managers may view broader workspace questions, answers, documents, usage metrics, feedback and review records than ordinary employee users, according to assigned permissions. Your organization controls invitations, membership and access assignments and may export authorized business information. We may access records when reasonably necessary to provide support, investigate incidents, protect the Service, meet legal obligations, or complete authorized requests.

Service access controls do not prevent an authorized person from copying or exporting information. Once your organization or another authorized recipient independently shares a copy outside the Service, that recipient's own practices also apply. OBIAnswers does not intentionally publish private workspace documents as public website content.

No sale or targeted advertising: We do not sell personal information, disclose it for cross-context behavioral advertising, or use it to serve targeted advertisements. We do not use workspace content for unrelated advertising. Provider disclosures described in this Policy support the Service and do not authorize those activities.

9. Cookies, local storage and analytics

The web Service uses session cookies and similar browser storage to authenticate users, maintain secure sessions and support account operations. Browser or device storage may also remember preferences such as theme, sign-in state or signup selections. Mobile applications use platform storage and authentication mechanisms for comparable functions. Blocking or clearing essential storage may sign you out or prevent functions from operating.

Where enabled, Vercel Web Analytics and Speed Insights measure page visits, technical characteristics and performance. Vercel describes Web Analytics as cookie-free; that does not mean all network processing is absent or that every security log is anonymous. Our account-link protections remove certain sensitive URL parameters from observability events and exclude the email-action page. Do not place confidential information in page URLs or voluntary feedback unnecessarily.

Use available browser, device and Service settings to manage storage and preferences. Those controls may not block essential server logs or security processing. Where legally required, optional tracking must be subject to appropriate notice and prior consent before use. Applicable opt-out preference signals, such as Global Privacy Control, will be honored for processing to which those requirements apply. We currently do not sell data or use targeted advertising, so there is no such activity to opt out of. A browser's general "Do Not Track" setting does not by itself disable all necessary processing.

10. International processing

ARGMEDIAGROUP LLC is based in the United States. Information may be processed in the United States and other countries where our providers operate, which may have different privacy laws from your country. Offering worldwide access is not a promise to keep information in your country or to have approval for every jurisdiction.

Transfers subject to mandatory restrictions require a valid legal mechanism and any additional required safeguards. Depending on the parties, locations and applicable law, these may include an adequacy decision or approved contractual safeguards. We do not rely merely on your use of the Service as consent to a restricted transfer. Contact us for the safeguards applicable to your processing; we will provide available information or a copy as required, subject to appropriate redaction. If required safeguards cannot be established, the affected processing must not proceed. We do not claim a privacy certification or transfer-framework participation merely because a provider holds one.

04 | STORAGE AND PROTECTION

Retention, security & younger users

11. Retention and deletion

Active accounts and workspace records. We retain information while needed to provide the Service, maintain the customer's knowledge and history, administer the account, and fulfill lawful customer instructions. Retention depends on the record type, account or subscription status, purpose, contractual instructions and legal requirements. Archiving a document is not permanent deletion; stored or failed files may remain until deleted.

Account closure. Personal account deletion removes account and membership records through the supported process, but does not automatically erase company documents, shared questions, answers, reviews, audit records, billing records, or information an organization must lawfully retain. A workspace owner may need to transfer ownership before using ordinary self-service account deletion. You can still contact us to exercise applicable privacy rights; ownership-transfer controls do not remove those rights.

After a workspace subscription ends. Under the standard customer agreement, the organization has 30 calendar days after termination to request retrieval. Unless earlier deletion is required or law permits or requires retention, active customer content is deleted or de-identified within 60 days after that retrieval period ends. Residual backups expire under the applicable schedule, no later than 180 days after termination except for a legal hold or legally required retention. These periods follow the accepted customer agreement and any lawful, specifically agreed DPA variation; they do not postpone a shorter mandatory legal duty.

Other records and providers. We retain billing and tax records as needed for applicable financial and tax requirements; support records while needed to resolve and document requests; and proportionate security, consent and dispute records as needed for their lawful purpose or applicable claim periods. Retained information remains protected and is not reused for unrelated purposes. Provider copies, files and derived indexes require relevant deletion steps; deleting a visible item may not instantly erase backups or legally retained security logs. We delete, de-identify or securely isolate information when its permitted retention purpose ends.

12. Security

We use safeguards intended to protect personal information, including server-side authorization, role and workspace restrictions, protected authentication sessions, encrypted network connections, restricted credentials, private storage rules and short-lived source access links. Access is limited according to operational duties. No system or transmission method is completely secure, and we cannot promise prevention of every incident. Please protect your account and device and promptly report suspected unauthorized access. Where required, we notify affected customers or individuals of security incidents under applicable law and contractual duties.

13. Children and younger employees

The Service is a business tool, not a service directed to children. Accounts for persons under 13 are prohibited. Subject to any higher local age requirement, employees aged 13-17 may use only eligible, supervised accounts after Company approval, any necessary minor-access addendum, and legally required notices, authorizations and safeguards. Permission to create a limited employee account does not authorize uploading unrelated children's records.

An employer invitation does not substitute for parental consent where required. The lawful basis, age threshold and required adult involvement depend on the jurisdiction and processing. We do not knowingly allow under-13 accounts. If you believe an ineligible child has supplied information, contact us so we can investigate, restrict affected processing and take appropriate deletion or protective action under applicable law. Information intended for younger users must be explained in language they can reasonably understand.

05 | REQUESTS AND CONTACT

Your rights, choices & policy updates

14. Privacy rights and requests

Depending on where you live, applicable thresholds, our role, and the nature of the information, you may have rights to confirm processing; access or obtain a copy; correct inaccurate data; delete data; receive portable information; restrict or object to processing; withdraw consent; or opt out of a sale, targeted advertising or certain profiling. These rights have lawful exceptions and do not apply identically everywhere. We do not make independent employment or similarly significant decisions about you solely through AI; customers remain responsible for their own decisions and lawful use.

Send requests to contact@argmediagroup.com with the subject "Privacy Request." Tell us what you want to exercise and provide enough information to locate the account or record. For customer-controlled workspace data, contact your organization first where practical; we will assist it or respond directly where our own duties require. We may verify identity and authority using proportionate measures and will not disclose another person's private records to satisfy an unverified request.

We will respond within the deadline required by applicable law, explain a lawful extension or refusal, and provide any required appeal instructions. Requests are generally free; charges or refusals apply only where law allows, such as certain manifestly unfounded or excessive requests. An authorized agent may act where permitted, with proof of authority and any necessary identity verification. We will not unlawfully discriminate or retaliate because you exercise privacy rights.

If you disagree with our response, email contact@argmediagroup.com with the subject "Privacy Appeal" and explain the concern. Where an appeal right applies, we will review it and respond within the applicable deadline. You may also complain to a competent privacy regulator or other authority; this process does not require you to waive that right. Where EU, EEA or UK data-protection law applies, you may complain to the relevant supervisory authority, including one in your habitual residence, workplace or place of alleged infringement where applicable.

15. Preferences and service communications

You may update available profile information and preferences in the Service. Where an application offers AI-processing controls, disabling a feature may prevent its further use on that application; it does not necessarily cancel the subscription, delete existing records, or change an organization's independent legal duties. Contact us if you need assistance. Withdrawal of consent does not affect the lawfulness of processing before withdrawal or processing that lawfully relies on another basis.

You may decline optional promotional messages through their unsubscribe mechanism or by contacting us. We may continue to send necessary account, security, billing, support and legal communications. Essential service messages are not marketing subscriptions. Browser and device settings can also control certain permissions and stored preferences.

16. Other services and changes to this Policy

Independent sites, app stores and services you choose to visit have their own privacy practices. This Policy describes OBIAnswers processing, not every activity of those third parties. Read their notices before sharing information.

We will update the date and version when this Policy changes and provide appropriate notice of material changes. Where a new use or disclosure requires consent, we will request it before that processing; a policy update alone does not create consent or retroactively waive rights. Contracts and DPAs govern their respective obligations, but cannot reduce mandatory privacy rights. This Policy does not assert that every jurisdictional requirement is satisfied merely by publishing it.

Questions or requests: contact@argmediagroup.com
ARGMEDIAGROUP LLC
111 Town Square Pl, Ste 1238, PMB 659533
Jersey City, New Jersey 07310-1810, United States