Privacy Policy

Effective date: October 19, 2026

At Azurite, we take your privacy seriously. Please read this Privacy Policy to learn how we treat your personal data. **By using or accessing our Services in any manner, you acknowledge that you accept the practices and policies outlined below, and you hereby consent that we will collect, use and share your information as described in this Privacy Policy.**

Remember that your use of Azurite's Services is at all times subject to our Terms of Use, which incorporates this Privacy Policy. Any terms we use in this Policy without defining them have the definitions given to them in the Terms of Use.

You may print a copy of this Privacy Policy using your browser's print function.

As we continually work to improve our Services, we may need to change this Privacy Policy from time to time. Upon such changes, we will alert you to material changes by placing a notice on the Azurite website, by sending you an email and/or by some other means. Please note that if you've opted not to receive legal notice emails from us (or you haven't provided us with your email address), those legal notices will still govern your use of the Services, and you are still responsible for reading and understanding them. If you use the Services after any changes to the Privacy Policy have been posted, that means you agree to all of the changes. If we change how we use Google User Data, we will notify you and ask for your consent before using your Google User Data in the new way.

Privacy Policy Table of Contents

- **What this Privacy Policy Covers**
- **Personal Data**
  - *Categories of Personal Data We Collect*
  - *Our Commercial or Business Purposes for Collecting or Disclosing Personal Data*
  - *Other Permitted Purposes for Processing Personal Data*
  - *Categories of Sources of Personal Data*
- **How We Disclose Your Personal Data**
- **Google User Data**
- **Tracking Tools, Advertising and Opt-Out**
- **Data Security**
- **Personal Data of Children**
- **U.S. State Privacy Rights**
- **Exercising Your Rights under U.S. State Privacy Laws**
- **Contact Information**

What this Privacy Policy Covers

This Privacy Policy covers how we treat Personal Data that we gather when you access or use our Services. "Personal Data" means any information that identifies or relates to a particular individual and also includes information referred to as "personally identifiable information" or "personal information" or "sensitive personal information" under applicable data privacy laws, rules or regulations. This Privacy Policy does not cover the practices of companies we don't own or control or people we don't manage.

Personal Data

Categories of Personal Data We Collect

This chart details the categories of Personal Data that we collect and have collected over the past 12 months:

Category of Personal Data (and Examples)	Business or Commercial Purpose(s) for Collection	Categories of Third Parties With Whom We Disclose this Personal Data
Profile or Contact Data such as first and last name, email address, and company name.	● Providing, Customizing and Improving the Services ● Corresponding with You	● Service Providers ● Parties You Authorize, Access or Authenticate
Identifiers such as unique identifiers associated with your account.	● Providing, Customizing and Improving the Services ● Corresponding with You	● Service Providers ● Parties You Authorize, Access or Authenticate
Payment Data such as payment information necessary to process your transactions, which is collected and processed directly by our payment processor.	● Providing, Customizing and Improving the Services ● Corresponding with You	● Service Providers (specifically our payment processing partner, Stripe, Inc.)
Commercial Data such as purchase history.	● Providing, Customizing and Improving the Services ● Corresponding with You	● Service Providers
Professional or Employment-Related Data such as job title, which is visible to members of your organization and may be provided to the AI model.	● Providing, Customizing and Improving the Services	● Service Providers
User Content such as prompts, files and documents you upload, data retrieved from third-party services you connect to the Services (for example, Google, QuickBooks, HubSpot or Slack), AI-generated outputs, reasons you provide when saving or merging changes, and the subject and message of support requests you submit.	● Providing, Customizing and Improving the Services	● Service Providers ● Parties You Authorize, Access or Authenticate
Device/IP Data and Web Analytics such as IP address, approximate location derived from IP address, device and browser type, operating system, a random installation identifier for our desktop app, pages viewed, buttons clicked, sign-up and checkout activity in our customer portal, the referring webpage or campaign, and whether you started or completed sign-up or a purchase after clicking one of our advertisements.	● Providing, Customizing and Improving the Services ● Marketing the Services	● Service Providers
Marketing Attribution Data such as the advertising campaign, referral link,	● Marketing the Services	● Service Providers

ad-click identifier, or random visit identifier that led you to sign up or request a demo, which we save with your account or with your demo request.		

Our Commercial or Business Purposes for Collecting Personal Data

- **Providing, Customizing and Improving the Services**
  - Creating and managing your account or other user profiles.
  - Processing orders or other transactions; billing.
  - Providing you with the products, services or information you request.
  - Meeting or fulfilling the reason you provided the information to us.
  - Providing support and assistance for the Services.
  - Improving the Services, including testing, research, internal analytics and product development.
  - Personalizing the Services, website content and communications based on your preferences.
  - Doing fraud protection, security and debugging.
  - Carrying out other business purposes stated when collecting your Personal Data or as otherwise set forth in applicable data privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020, the Colorado Privacy Act, the Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, the Indiana Consumer Data Protection Act, the Iowa Consumer Data Protection Act, the Kentucky Consumer Data Protection Act, the Maryland Online Data Privacy Act, the Minnesota Consumer Data Privacy Act, the Montana Consumer Data Privacy Act, the New Hampshire Privacy Act, the New Jersey Privacy Act, the Nebraska Data Privacy Act, the Oregon Consumer Privacy Act, the Rhode Island Data Transparency and Privacy Protection Act, the Tennessee Information Protection Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, or the Virginia Consumer Data Protection Act (collectively, the "U.S. State Privacy Laws").
- **Marketing the Services**
  - Marketing and selling the Services.
  - Measuring the effectiveness of our advertising campaigns.
- **Corresponding with You**
  - Responding to correspondence that we receive from you, contacting you when necessary or requested, and sending you information about Azurite or the Services.
  - Sending emails and other communications according to your preferences.

Other Permitted Purposes for Processing Personal Data

In addition, each of the above referenced categories of Personal Data may be collected, used, and disclosed with the government, including law enforcement, or other parties to meet certain legal requirements and enforcing legal terms including: fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal or prohibited activities; protecting the rights, property or safety of you,

Azurite or another party; enforcing any agreements with you; responding to claims that any posting or other content violates third-party rights; and resolving disputes.

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated or incompatible purposes without providing you notice or obtaining your consent.

Categories of Sources of Personal Data

We collect Personal Data about you from the following categories of sources:

- **You**
  - When you provide such information directly to us.
    - When you create an account or use our interactive tools and Services.
    - When you voluntarily provide information in free-form text boxes through the Services or through responses to surveys or questionnaires.
    - When you send us an email or otherwise contact us.
  - When you use the Services and such information is collected automatically.
    - Through Cookies and similar technologies, such as browser storage and analytics tools (described in the "Tracking Tools, Advertising and Opt-Out" section below).
    - If you install our desktop application, it sends us information used to provide updates, including a random installation identifier, the app version, and your operating system and device architecture.
  - Third-Party Credentials

    If you sign in with Google or connect a Google service, please see the "Google User Data" section below for how we handle that data. If you connect other third-party services, such as QuickBooks, HubSpot or Slack, some content and information from those accounts may be transmitted into your account with us. When you ask, the Services can also take actions in connected services on your behalf, such as sending email or posting messages. By default, Azurite asks for your approval before taking these actions, and automated background runs cannot take them. If you change your settings to always allow an action, Azurite, including automated background runs, may take that action without asking you first.

How We Disclose Your Personal Data

We disclose your Personal Data to the categories of service providers and other parties listed in this section. We do not sell your Personal Data or share it for cross-context behavioral advertising. For more information, please refer to the state-specific sections below.

- **Service Providers.** These parties help us provide the Services or perform business functions on our behalf. They include:

- Hosting, technology and communication providers (currently including Amazon Web Services and, for our website, Neon and Resend).
- Analytics providers for web traffic or usage of our Services (currently PostHog).
- Spam and abuse prevention providers (currently Cloudflare).
- Support and customer service vendors, including Linear, which receives bug reports you submit through the Services, including your name and email address, information about your device, an excerpt of your recent session activity, and any screenshots you attach, and Slack, which we use to notify our team of new support requests and which receives a shortened version of the request's subject and your organization's name, plan and billing status, but not your email address or the message itself.
- Payment processors.
    - Our payment processing partner Stripe, Inc. ("Stripe") collects your voluntarily-provided payment card information necessary to process your payment.
    - Please see Stripe's terms of service and privacy policy for information on its use and storage of your Personal Data.
- Artificial intelligence processing providers. When you use AI-powered features of the Services, content such as your prompts, files, data retrieved from connected services, and model responses is sent to OpenRouter, Inc. ("OpenRouter"), an AI routing provider, which passes it to a provider that hosts the model being used, which may be the model's developer or a third-party hosting provider. Models available in our Services include those developed by Anthropic, PBC (Claude), OpenAI (GPT), Google (Gemini), Moonshot AI (Kimi) and Z.ai (GLM). We configure OpenRouter to route requests only to providers that, according to OpenRouter, do not collect user data. We also send parts of requests, such as system instructions and tool definitions, directly to Anthropic, PBC to count the tokens in a request, which we use to manage request size, and we use Amazon Bedrock, provided by Amazon Web Services, to build search indexes of content you save and to rank search results. When you use web search features, search queries written by the AI model are sent to Brave Software, Inc. ("Brave Search"). Please review the privacy policies of these providers for more information.
- Your main chat history is stored on your device. Some features send content to our servers and to the AI providers described above, and if you submit a bug report, an excerpt of your recent session activity is sent to Linear, as described above. For example, when you merge an edit into your organization's project, we keep the new file versions and a change-history entry that an AI model writes from the file changes and your chat. We send your chat history to our AI provider only to write that entry, and we delete our server copy of it afterward. If you submit a merge request for approval, we keep your chat history and stated reason until the request is approved, rejected or cancelled, and an AI-written summary of the request may be retained. We also store searchable summaries of your artifacts and knowledge terms; we keep records of tasks for 30 days and batch records for 90 days; we keep automation results and a record of each automation step until you delete the automation or your organization's account is deleted; and we keep the raw data an automation receives from connected services for 90 days. This and other server-side data, such as automation outputs and connector records, is protected by credentialed access controls governing Azurite's database and cloud storage.

- **Parties You Authorize, Access or Authenticate**
    - Third parties you access through the services.

Legal Obligations

We may disclose any Personal Data that we collect with third parties in conjunction with any of the activities set forth under "Other Permitted Purposes for Processing Personal Data" section above.

Business Transfers

All of your Personal Data that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part).

Data that is Not Personal Data

We may create aggregated, de-identified or anonymized data from the Personal Data we collect, including by removing information that makes the data personally identifiable to a particular user. We may use such aggregated, de-identified or anonymized data and disclose it with third parties for our lawful business purposes, including to analyze, build and improve the Services and promote our business, provided that we will not attempt to reidentify the data and/or disclose such data in a manner that could identify you.

Google User Data

This section describes how Azurite handles information we receive from Google APIs ("Google User Data"). Notwithstanding anything else in this Privacy Policy, our use, disclosure and retention of Google User Data is limited as described in this section.

Google User Data we access. We access Google User Data only when you sign in with Google or connect a Google service, and only from the service you connect:

- **Google sign-in:** your name, email address and basic profile information, to create your account and sign you in.
- **Gmail:** permission to read, organize and send your email, and to manage your Gmail filters and vacation auto-reply. We use it to search and read the messages and attachments you ask about and, when you ask, to organize your email with labels, move messages to Trash and restore them, create, send and forward email and drafts, and manage your filters and vacation auto-reply. By default, Azurite asks for your approval before it changes, sends or deletes anything in your Gmail.
- **Google Drive:** permission to see, edit, create and delete your Google Drive files. We use it to find and read the files you ask about, including meeting notes and attendance reports that Google Meet saves to your Drive, and, when you ask, to create, copy, edit, rename and move files, move them to Trash and restore them, edit Google Docs and Sheets, add and reply to comments, and share files or change who can access them, including sharing by link and transferring ownership. By default, Azurite asks for your approval before it changes, shares or trashes a file.
- **Google Meet:** permission to create meetings, manage the meetings Azurite creates, change the settings of your meetings, and read information about meetings you can access. We use it, when you ask, to create meetings, change their settings and host controls, end a call in progress, and add or

remove co-hosts and guests, and to read the participants and transcripts of your meetings and the details of their recordings and meeting notes. Azurite reads the text of meeting notes and attendance reports only through Google Drive, if you connect it. By default, Azurite asks for your approval before it changes a meeting.

How we use Google User Data. We use Google User Data only to provide the features of the Services described above. We do not sell it, use it for advertising, or use it to determine creditworthiness or for lending purposes.

Who we share Google User Data with. We share Google User Data only (1) with the people you choose, when you ask Azurite to send or forward an email or share a file; (2) with our service providers, including the AI providers described in "Service Providers" above, to deliver a feature you asked for; (3) for security purposes, such as investigating abuse; (4) to comply with applicable law; or (5) as part of a merger, acquisition or sale of assets, after obtaining your explicit prior consent. We never transfer it to advertising platforms, data brokers or information resellers.

Staff access. Azurite staff do not read Google User Data unless (1) you give us explicit consent to view specific data, for example by submitting a bug report that includes your recent conversation; (2) it is necessary for security purposes, such as investigating a bug or abuse; (3) it is necessary to comply with applicable law; or (4) the data is aggregated and anonymized and used for internal operations.

AI models. Azurite does not use Google User Data to develop, improve or train generalized or non-personalized artificial intelligence or machine learning models, and we configure OpenRouter, our AI routing provider, to exclude providers that train on request data.

Storage, protection, retention and deletion. Your main chat history is stored on your device. It keeps the AI model's replies, which may quote or summarize Google User Data, but not the Google User Data the AI model retrieves. Some features send content, which may include Google User Data, to our servers and to the AI providers described in "Service Providers" above. We do not copy Google User Data into our file storage or search indexes, except that when an automation reads Google User Data on our servers, we keep the full results for up to 90 days and a record of each step until you delete the automation. Google User Data stored on our servers is encrypted at rest, Google access tokens are separately encrypted before they are stored, and access is limited by credentialed access controls governing Azurite's database and cloud storage. We keep your Google access tokens until you disconnect the service, leave your organization, or your organization closes its account, and then we delete them. When you disconnect a Google service, we also delete the automation results and the Google User Data in automation records for that service, and when you disconnect the last Google service you have connected, we revoke Azurite's access with Google. Content you save is kept until you delete it or your organization closes its account, and we delete an organization's data within 60 days after it closes. You can ask us to delete your Google User Data at any time by emailing Support@azuriteintelligence.com, and we will do so within 30 days.

Azurite's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Gmail, Google Drive and Google Meet are trademarks of Google LLC.

Tracking Tools, Advertising, and Opt-Out

The Services use cookies and similar technologies such as browser storage and JavaScript (collectively, "Cookies") as described below. Our public website does not set advertising or analytics cookies. It uses limited browser storage and third-party scripts, and a fraud-prevention cookie set by our payment processor, each as described below. Other parts of the Services, such as signed-in areas, may use cookies that are strictly necessary to log you in. Cookies are small pieces of data– usually text files – placed on your computer, tablet, phone or similar device when you use that device to access our Services. We may also supplement the information we collect from you with information received from third parties, including third parties that have placed their own Cookies on your device(s).

We use the following types of Cookies:

- Essential Cookies. Essential Cookies are required for providing you with features or services that you have requested. For example, certain Cookies enable you to log into secure areas of our Services. Disabling these Cookies may make certain features and services unavailable.
- Analytics. We use PostHog to understand how visitors use our website, such as which pages are viewed and which buttons are clicked. We configure PostHog in a cookieless mode, so it does not place cookies on your device or store identifiers in your browser. PostHog receives page views, clicks, referrer and campaign (UTM) information, any ad-click identifiers included in the page address, device and browser details, and a random identifier we add to sign-up links so we can tell which visit led to an account. PostHog also receives your IP address and uses it to derive your approximate location. PostHog processes this data on our behalf in the United States. Our website does not use PostHog for visitors from the European Economic Area, the United Kingdom or Switzerland, as described below. When you create an account after arriving from one of our campaigns or referral links, our servers send PostHog a record that the account was created, without your IP address or location.
- Account and Checkout Analytics. When you sign up for or purchase the Services through our customer portal, we record events in PostHog, such as when you start, complete or cancel sign-up or checkout, the plan and billing period you choose, whether you signed in with Google or by email, error codes, the checkout price and currency, and the advertising campaign that led you to us, so that we can understand how customers sign up for and purchase the Services. These events do not include your name, email address, company name or payment card information, and we do not send your IP address or location with them. Our customer portal does not set cookies. It uses your browser's session storage, which is cleared when you close the tab or sign out, to keep a random identifier and your plan and campaign selections between steps. We do not record these events or store this information for users in the European Economic Area, the United Kingdom or Switzerland, or whose location we cannot determine.
- Browser Storage and Security Tools. While you browse, we keep your campaign and referrer information in your browser's session storage until you close the tab, so we can tell which campaign led you to us. We do not do this for visitors from those regions. Our forms use Cloudflare Turnstile to detect automated abuse, which loads a script from Cloudflare when a form is shown. We use Stripe to process payments. Stripe's script on our website sets a cookie (__stripe_mid) that Stripe uses to detect and prevent fraud, and payments are completed on pages hosted by Stripe, which sets its own cookies under its own policy.
- Advertising. We advertise the Services through Google Ads, provided by Google LLC ("Google"). When you start sign-up for the Services, complete sign-up for an individual account, or complete a purchase of a Teams plan, our customer portal loads a Google Ads conversion tag from our main website in a hidden frame. The tag does not set a cookie on your device; it tells Google that the sign-up or purchase occurred, so that we can measure which of our advertisements lead to sign-ups

and purchases. Google also receives your IP address, as with any connection to Google, and, when you start sign-up, the Google ad click identifier from the advertisement you clicked. The tag runs only on our main website and does not run within our customer portal itself. We have enabled Google's restricted data processing setting, under which Google uses this information only to measure our advertising on our behalf and not to personalize advertising. We do not load this tag for visitors from the European Economic Area, the United Kingdom or Switzerland, for visitors whose location we cannot determine, or for visitors whose browser sends a Global Privacy Control signal.

You can decide whether or not to accept Cookies through your internet browser's settings. Most browsers have an option for turning off the Cookie feature, which will prevent your browser from accepting new Cookies, as well as (depending on the sophistication of your browser software) allow you to decide on acceptance of each new Cookie in a variety of ways. You can also delete all Cookies that are already on your device. If you do this, however, you may have to manually adjust some preferences every time you visit our website and some of the Services and functionalities may not work.

If you visit our website from the European Economic Area, the United Kingdom or Switzerland, or if we cannot determine your location, we do not use the analytics, session storage or advertising tag described above, and we do not save campaign or referral information with your account or demo request. To decide this, our website asks our own server for your country based on your IP address. This information is not stored or shared. Our public website does not set advertising or analytics cookies, and you can control cookies in your browser settings. If we add tools that need your consent, we will update this Privacy Policy first. To find out more information about Cookies generally, including information about how to manage and delete Cookies, please visit http://www.allaboutcookies.org/

Data Security

We seek to protect your Personal Data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of Personal Data and how we are processing that data. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism; limiting access to your computer or device and browser; and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

Data Retention

We retain Personal Data about you for as long as necessary to provide you with our Services or to perform our business or commercial purposes for collecting your Personal Data. When establishing a retention period for specific categories of data, we consider who we collected the data from, our need for the Personal Data, why we collected the Personal Data, and the sensitivity of the Personal Data. We may further retain information in an anonymous or aggregated form where that information would not identify you personally. We may retain your data as necessary to comply with legal obligations, resolve disputes, or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation. Records of tasks are kept for 30 days and batch records for 90 days. Automation results and a record of each automation step are kept until you delete the automation or your organization's account is deleted, and the raw data an automation receives from connected services is kept for 90 days. When we delete your account, we also delete your sign-in records. We keep billing, payment and usage records, such as

your organization's billing contact and records of its use of the Services, in business systems that are separate from your organization's account data. These records are not removed when your account or your organization's account is deleted, and we use them for accounting, tax, audit and dispute-resolution purposes. You may request deletion of these records as described in "U.S. State Privacy Rights," subject to any records we are required by law to keep. If your organization closes its account, we delete its account data within 60 days, except the records described in this paragraph. Support requests are kept while we need them to respond to you and support your account, and support requests tied to an organization are deleted when that organization's account is deleted. Audit-trail entries created when you save or merge changes are retained as part of your organization's records.

Personal Data of Children

As noted in the Terms of Use, we do not knowingly collect or solicit Personal Data from individuals under 18 years of age; if you are under the age of 18, please do not attempt to register for or otherwise use the Services or send us any Personal Data. If we learn we have collected Personal Data from individuals under 18 years of age, we will delete that information in accordance with applicable law. If you believe that a User under 18 years of age may have provided Personal Data to us, please contact us at Support@azuriteintelligence.com.

U.S. State Privacy Rights

If you reside in certain U.S. states such as California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia you may have certain rights afforded to you (as described below) depending on your state of residence. Please see the 'Exercising Your Rights under U.S. State Privacy Laws' section below for instructions regarding how to exercise these rights. Please note that we may process Personal Data of our customers' end users or employees in connection with our provision of certain services for our customers. If we are processing your Personal Data as a service provider, you should contact the entity that collected your Personal Data in the first instance to address your rights with respect to such data. Please note that your rights may be subject to certain conditions or exceptions in accordance with applicable U.S. State Privacy Laws.

If you have any questions about this section or whether any of the following rights apply to you, please contact us at Support@azuriteintelligence.com.

- *Access*: You may have the right to request confirmation of or access to the Personal Data that we process about you. You can also request access to a portable copy of your Personal Data. If you are a Minnesota or Oregon resident, you also have the right to request a list of specific third parties, other than natural persons, to whom we have disclosed your Personal Data (subject to exceptions in accordance with applicable law).
- *Deletion*: You may have the right to request that we delete the Personal Data that we have collected about you.
- *Correction*: You may have the right to request that we correct any inaccurate Personal Data we have collected about you.
- *Portability*: You may have the right to request a copy of your Personal Data in a machine-readable format, to the extent technically feasible.

Anti-Discrimination

We will not discriminate against you for exercising your rights under applicable privacy laws. We will not deny you our goods or services, charge you different prices or rates, or provide you a lower quality of goods and services if you exercise your rights under applicable privacy laws. However, we may offer different tiers of our Services as allowed by applicable data privacy laws with varying prices, rates or levels of quality of the goods or services you receive related to the value of Personal Data that we receive from you.

Other State-Specific Privacy Rights

Under California Civil Code Sections 1798.83-1798.84, California residents are entitled to contact us to prevent disclosure of Personal Data to third parties for such third parties' direct marketing purposes; in order to submit such a request, please contact us at Support@azuriteintelligence.com.

Your browser may offer you a "Do Not Track" option, which allows you to signal to operators of websites and web applications and services that you do not wish such operators to track certain of your online activities over time and across different websites. Our Services do not support Do Not Track requests at this time. To find out more about "Do Not Track," you can visit www.allaboutdnt.com.

If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties. You can exercise this right by contacting us at Support@azuriteintelligence.com with the subject line "Nevada Do Not Sell Request" and providing us with your name and the email address associated with your account. Please note that we do not currently sell your Personal Data as sales are defined in Nevada Revised Statutes Chapter 603A.

Exercising Your Rights under U.S. State Privacy Laws

To exercise the rights described in this Privacy Policy, you or your Authorized Agent (if applicable and as defined below), must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected Personal Data (such as your Contact or Profile Data), and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a "Valid Request." We may not respond to requests that do not meet these criteria. We will only use Personal Data provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within the time period required by applicable privacy laws. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

Request to Access, Delete, Correct

As applicable, you may submit a Valid Request for your right to access, delete, correct, or obtain a copy of your Personal Data described in this Privacy Policy by using the following methods:

- Email us at: Support@azuriteintelligence.com
- Call us at: 775-525-0298
- Submit a form at this address: 455 West Evelyn Ave STE 2202, Mountain View, CA, 94041

If you are a California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey Oregon, Rhode Island, or Texas resident, you may also authorize an agent (an "Authorized Agent") to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf.

Appealing a Denial

If you are a Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, or Virginia resident and we refuse to take action on your request within a reasonable period of time after receiving your request in accordance with this section, you may appeal our decision. In such appeal, you must (1) provide sufficient information to allow us to verify that you are the person about whom the original request pertains and to identify the original request, and (2) provide a description of the basis of your appeal. Please note that your appeal will be subject to your rights and obligations afforded to you under the U.S. State Privacy Laws (as applicable). We will respond to your appeal within the time period required under the applicable law. You can submit a Verified Request to appeal by the following methods:

- Email us at: Support@azuriteintelligence.com (title must include "[STATE OF RESIDENCE] Appeal")
- Call us at: 775-525-0298
- Submit a form at this address: 455 West Evelyn Ave STE 2202, Mountain View, CA, 94041

If we deny your appeal, you have the right to contact the Attorney General of your State, including by the following links: Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, and Virginia.

Contact Information:

If you have any questions or comments about this Privacy Policy, the ways in which we collect and use your Personal Data or your choices and rights regarding such collection and use, please do not hesitate to contact us at:

- 775-525-0298
- Support@azuriteintelligence.com
- 455 West Evelyn Ave STE 2202, Mountain View, CA 94041