InboxBrief — Google User Data Privacy Policy

Version 3.0 | Effective Date: March 21, 2026 | Last Reviewed: March 21, 2026

Preamble

This Google User Data Privacy Policy ("Google Policy") is a supplement to InboxBrief's main Privacy Policy and governs InboxBrief's access to, use of, storage of, and disclosure of data obtained through Google APIs, including the Gmail API, Google OAuth 2.0, and related Google Workspace APIs. This Google Policy is required by and consistent with the Google API Services User Data Policy (https://developers.google.com/terms/api-services-user-data-policy) and the Google Workspace API User Data and Developer Policy (https://developers.google.com/workspace/workspace-api-user-data-developer-policy).

By connecting your Google account to InboxBrief, you acknowledge that you have read, understood, and agree to the terms of this Google Policy. If you do not agree to this Google Policy, you must not connect your Google account to InboxBrief.

InboxBrief's use of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. This statement is required by Google and is incorporated into InboxBrief's Privacy Policy as a standalone disclosure.

Section 1 — Google API Services Used

InboxBrief uses the following Google API services:

1.1 Gmail API

InboxBrief uses the Gmail API to access your Gmail inbox for the purpose of generating personalized email briefings. The Gmail API allows InboxBrief to read email metadata and content from your inbox. InboxBrief does not use the Gmail API to send emails, delete emails, modify emails, or access any Gmail feature beyond reading your inbox.

1.2 Google OAuth 2.0

InboxBrief uses Google OAuth 2.0 for user authentication and to obtain authorized access to the Gmail API on your behalf. Google OAuth 2.0 allows you to grant InboxBrief access to your Google account without sharing your Google password with InboxBrief.

1.3 Google People API (Profile Data)

InboxBrief uses the Google People API to retrieve your basic profile information (name, email address, and profile picture URL) at the time of account creation. This information is used to populate your InboxBrief account profile.

Section 2 — Gmail API Scopes Requested

InboxBrief requests the following Gmail API OAuth scopes when you connect your Google account:

Scope	Description	Why InboxBrief Needs It
`https://www.googleapis.com/auth/gmail.readonly`	Read-only access to Gmail messages and metadata	To fetch email metadata (sender, subject, snippet) for briefing generation
`https://www.googleapis.com/auth/userinfo.email`	View your email address	To identify your Gmail account and associate it with your InboxBrief account
`https://www.googleapis.com/auth/userinfo.profile`	View your basic profile info	To populate your InboxBrief account name and profile picture

InboxBrief does not request and will never request the following scopes: `gmail.modify`, `gmail.compose`, `gmail.send`, `gmail.insert`, `gmail.labels`, `gmail.settings.basic`, `gmail.settings.sharing`, `mail.google.com` (full access), or any scope that would allow InboxBrief to modify, delete, or send email on your behalf.

Section 3 — What Google Data InboxBrief Accesses

When you connect your Gmail account, InboxBrief accesses the following data from your Gmail inbox:

3.1 Email Metadata

For each email in your inbox, InboxBrief accesses:

- **Sender name and email address**: Used to identify who sent the email and to classify its priority level.
- **Subject line**: Used to understand the topic of the email and to generate a meaningful briefing entry.
- **Email snippet**: A short excerpt (up to 300 characters) of the email body, used to provide context for AI classification and briefing generation.
- **Received timestamp**: Used to identify new emails since the last briefing.
- **Message ID**: Used to track which emails have already been processed (incremental fetching) to avoid duplicate briefing entries.

3.2 What InboxBrief Does NOT Access

InboxBrief does not access, read, store, or process the following Gmail data:

- Full email body content beyond the 300-character snippet
- Email attachments (files, images, documents)
- Email drafts
- Sent mail
- Spam or trash folders
- Email labels or categories
- Gmail settings or filters
- Contact lists
- Calendar data
- Google Drive files
- Any other Google service data

Section 4 — How InboxBrief Uses Google User Data

InboxBrief uses Google user data exclusively for the following purposes, consistent with the Google API Services User Data Policy Limited Use requirements:

4.1 Permitted Uses

Email Briefing Generation: InboxBrief uses email metadata (sender, subject, snippet) to generate AI-powered SMS briefings that summarize your inbox. This is the primary and essential purpose for which InboxBrief accesses your Gmail data.

Email Classification: InboxBrief uses email metadata to classify emails as high-priority, general, or low-priority using AI. This classification determines which emails are included in your briefing.

Incremental Fetching: InboxBrief uses Gmail Message IDs to track which emails have already been processed, ensuring that each email appears in only one briefing and that briefings contain only new emails since the last delivery.

Account Association: InboxBrief uses your Google email address to associate your Gmail account with your InboxBrief account and to prevent duplicate account creation.

4.2 Prohibited Uses — Limited Use Policy Compliance

InboxBrief strictly adheres to the Google API Services User Data Policy Limited Use requirements. InboxBrief does not:

- Use Gmail data for advertising purposes or to serve targeted advertisements
- Use Gmail data to train machine learning models, including AI models used by InboxBrief or any third party
- Transfer Gmail data to third parties except as strictly necessary to provide the email briefing service (specifically, transmitting email snippets to OpenRouter for AI processing, as described in Section 6)
- Allow human access to Gmail data except as required for security investigations, legal compliance, or with your explicit consent
- Use Gmail data for any purpose other than the email briefing service you have explicitly requested
- Combine Gmail data with data from other sources for purposes unrelated to the email briefing service
- Sell, rent, or otherwise monetize Gmail data

Section 5 — Storage and Security of Google User Data

5.1 OAuth Token Storage

When you connect your Gmail account, Google provides InboxBrief with an OAuth access token and a refresh token. These tokens are used to access your Gmail inbox on your behalf. InboxBrief stores these tokens in the following manner:

Both the access token and the refresh token are encrypted using AES-256-GCM encryption with a 256-bit key before being written to InboxBrief's database. A unique, randomly generated initialization vector (IV) is used for each encryption operation, ensuring that even identical tokens produce different ciphertext. The encryption key is stored separately from the encrypted tokens and is never stored in the database. Encrypted tokens are stored in InboxBrief's TiDB Cloud database, which itself encrypts all data at rest.

5.2 Email Metadata Processing

Email metadata (sender, subject, snippet) retrieved from the Gmail API is processed in memory to generate your briefing. Email metadata is transmitted to OpenRouter's API for AI processing (as described in Section 6) and is then discarded from InboxBrief's active memory. InboxBrief stores only the AI-generated briefing summary, not the raw email metadata, in encrypted form in its database.

5.3 Access Controls

Access to Gmail data is restricted to the automated InboxBrief server processes that perform email fetching and briefing generation. No InboxBrief employee has routine access to your Gmail data, OAuth tokens, or email metadata. Administrative access to InboxBrief's production database requires multi-factor authentication and is logged for audit purposes.

5.4 Data Minimization

InboxBrief applies the principle of data minimization to all Google user data processing. InboxBrief requests only the minimum Gmail API scopes necessary to deliver the email briefing service, accesses only the email metadata necessary to generate a meaningful briefing, retains email metadata only for the duration of the

briefing generation process, and stores only the AI-generated briefing summary (not raw email data) in its database.

Section 6 — Disclosure of Google User Data to Third Parties

InboxBrief discloses Google user data to the following third parties, solely as necessary to provide the email briefing service:

6.1 OpenRouter, Inc. (AI Processing)

InboxBrief transmits email metadata (sender name, subject line, and email snippet up to 300 characters) to OpenRouter's API for AI-powered email classification and briefing generation. This transmission is necessary to generate your briefing. OpenRouter processes this data solely to fulfill InboxBrief's API request and does not retain the data after the API call completes. OpenRouter does not use InboxBrief's submitted data to train AI models.

InboxBrief has reviewed OpenRouter's data processing practices and has determined that they are consistent with the Google API Services User Data Policy Limited Use requirements. OpenRouter's Privacy Policy is available at https://openrouter.ai/privacy.

6.2 No Other Third-Party Disclosures

InboxBrief does not disclose your Gmail data to any other third party, including Twilio (which receives only the AI-generated briefing text, not raw email data), Stripe (which receives only payment information), or any advertising network, data broker, or analytics provider.

6.3 Legal Disclosures

InboxBrief may disclose Google user data if required by applicable law, court order, or governmental authority. In such cases, InboxBrief will provide you with prompt notice of the disclosure requirement to the extent permitted by law.

Section 7 — Your Rights Regarding Google User Data

7.1 Revoking Access

You may revoke InboxBrief's access to your Gmail account at any time through either of the following methods:

Through InboxBrief: Navigate to your InboxBrief account settings, locate the "Connected Accounts" section, and click "Disconnect" next to your Gmail account. InboxBrief will immediately delete your stored OAuth tokens and cease all Gmail API access.

Through Google: Navigate to https://myaccount.google.com/permissions, locate InboxBrief in the list of connected apps, and click "Remove Access." This immediately revokes InboxBrief's OAuth tokens, preventing any further Gmail API access.

After revocation, InboxBrief will delete your stored OAuth tokens within 24 hours and will cease all Gmail API access immediately upon token revocation.

7.2 Data Deletion

Upon disconnecting your Gmail account or deleting your InboxBrief account, InboxBrief will delete all stored Gmail OAuth tokens and all briefing summaries generated from your Gmail data within 30 days. InboxBrief will retain only anonymized usage statistics (e.g., total number of briefings generated) that cannot be linked to your identity.

7.3 Access to Your Data

You may request a copy of all data InboxBrief holds about your Gmail account by contacting support@inboxbrief.com. InboxBrief will provide a machine-readable export within 30 days of receiving your request.

Section 8 — Google's Verification and Audit Rights

InboxBrief acknowledges that Google has the right to verify InboxBrief's compliance with the Google API Services User Data Policy and the Google Workspace API User Data

and Developer Policy. InboxBrief agrees to cooperate with any Google audit or verification process, including providing access to InboxBrief's data handling practices, technical documentation, and security assessments.

InboxBrief undergoes periodic security assessments of its Gmail API integration to ensure continued compliance with Google's requirements. InboxBrief will promptly notify Google of any security incident that may have resulted in unauthorized access to Google user data.

Section 9 — Compliance with Google's Limited Use Policy

InboxBrief's Gmail API integration complies with all requirements of the Google API Services User Data Policy Limited Use Policy. Specifically:

InboxBrief uses Gmail data only to provide or improve the user-facing features of the email briefing service that the user has explicitly requested. InboxBrief does not use Gmail data for any purpose that is not directly related to providing the email briefing service. InboxBrief does not transfer Gmail data to third parties except as necessary to provide the email briefing service (OpenRouter AI processing) or as required by law. InboxBrief does not allow humans to read Gmail data unless the user has given explicit consent, it is necessary for security investigations, or it is required by law. InboxBrief does not use Gmail data to build user profiles for advertising purposes. InboxBrief does not use Gmail data to train AI models.

The required Limited Use disclosure statement is: **"InboxBrief's use of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements."**

Section 10 — Google Workspace API Compliance

For users who connect a Google Workspace (formerly G Suite) account, InboxBrief's Gmail API integration complies with the Google Workspace API User Data and Developer Policy. InboxBrief provides the following disclosures required by that policy:

Data Access Disclosure: InboxBrief accesses Gmail message metadata (sender, subject, snippet) and Gmail Message IDs from your Google Workspace inbox. InboxBrief does not access any other Google Workspace data.

Data Collection Disclosure: InboxBrief collects Gmail OAuth tokens (encrypted), Gmail Message IDs (for incremental fetching), and AI-generated briefing summaries derived from Gmail metadata.

Data Use Disclosure: InboxBrief uses Gmail data solely to generate personalized email briefings delivered via SMS. InboxBrief does not use Gmail data for advertising, model training, or any purpose unrelated to the email briefing service.

Data Sharing Disclosure: InboxBrief shares Gmail metadata (sender, subject, snippet) with OpenRouter, Inc. solely for AI processing to generate briefings. InboxBrief does not share Gmail data with any other third party.

Section 11 — Security Assessment and Certification

InboxBrief is committed to maintaining the security of Google user data. InboxBrief implements the following security measures specifically for Google user data:

AES-256-GCM encryption for all stored OAuth tokens, with unique initialization vectors per encryption operation. TLS 1.2 or higher for all data in transit between InboxBrief's servers and Google's APIs. Strict access controls limiting Gmail API access to authorized server processes only. Automated token refresh with immediate deletion of expired tokens. Security incident response procedures that include immediate revocation of compromised OAuth tokens. Regular security reviews of the Gmail API integration.

For applications accessing sensitive or restricted Gmail API scopes, Google may require a third-party security assessment. InboxBrief will comply with any Google-mandated security assessment requirements and will make the results of such assessments available to Google upon request.

Section 12 — Changes to This Google Policy

InboxBrief reserves the right to modify this Google User Data Privacy Policy at any time. We will provide notice of material changes by posting the updated Policy on this page with a revised “Last Reviewed” date and by sending an email notification to users who have connected a Gmail account. Your continued use of the Gmail integration after the effective date of any changes constitutes your acceptance of the revised Policy.

If changes to this Policy would result in InboxBrief using Gmail data in a manner inconsistent with the Google API Services User Data Policy, InboxBrief will obtain your explicit consent before implementing such changes.

Section 13 — Contact Information

For questions, concerns, or requests related to this Google User Data Privacy Policy or InboxBrief’s use of Google user data, please contact:

InboxBrief Privacy Team Email: support@inboxbrief.com Website: https://inboxbrief.org/privacy

For urgent matters related to Google user data, please use the subject line “GOOGLE DATA PRIVACY” in your email communication. InboxBrief will respond to all Google data privacy inquiries within 5 business days.

This Google User Data Privacy Policy was last reviewed and updated on March 21, 2026. InboxBrief is committed to responsible use of Google user data and to full compliance with Google’s API Services User Data Policy.