# InboxBrief — Privacy Policy

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

## Preamble

This Privacy Policy ("Policy") describes how InboxBrief ("Company," "we," "us," or "our") collects, uses, stores, discloses, and protects personal information about users ("you" or "your") of the InboxBrief platform, including all associated websites, applications, APIs, and related services (collectively, the "Service"). This Policy applies to all users of the Service, regardless of geographic location, and supplements any jurisdiction-specific disclosures set forth in the appendices to this Policy.

InboxBrief is committed to protecting your privacy and to being transparent about its data practices. This Policy is designed to help you understand what data we collect, why we collect it, how we use it, with whom we share it, and what rights you have with respect to your personal data. We encourage you to read this Policy carefully and to contact us at support@inboxbrief.com if you have any questions.

This Policy should be read in conjunction with InboxBrief's Terms of Service and, for users who connect a Google account, InboxBrief's Google User Data Privacy Policy, both of which are available at https://inboxbrief.org/privacy.

## Section 1 — Information We Collect

### 1.1 Information You Provide Directly

InboxBrief collects the following categories of information that you provide directly when registering for or using the Service:

**Account Registration Data** includes your name, email address, and any other information you provide when creating your InboxBrief account through our OAuth-

based registration process.

**Onboarding Data** includes your business type, email volume estimate, primary business goal, and other qualifying information you provide during the onboarding process. This information is used to personalize your briefing experience and to tailor our service recommendations.

**Contact Information** includes your mobile phone number, which is required to receive SMS briefings. Your phone number is verified via one-time passcode (OTP) before first use and is stored in encrypted form.

**Payment Information** is collected by our payment processor, Stripe, Inc., when you subscribe to a paid plan. InboxBrief does not directly collect or store your payment card numbers, CVV codes, or bank account information. InboxBrief receives only a Stripe Customer ID and Stripe Subscription ID from Stripe.

**Preferences and Settings** include your briefing schedule preferences (time, frequency, timezone), language preference, keyword filters, tone preferences, and other customization settings you configure in the Service.

**Feedback and Communications** include ratings, comments, and other feedback you provide about your briefings, as well as communications you send to InboxBrief's support team.

## 1.2 Information Collected Automatically

When you access or use the Service, InboxBrief automatically collects certain technical information:

**Log Data** includes your IP address, browser type and version, operating system, referring URLs, pages viewed, time spent on pages, and other diagnostic information. Log data is retained for up to 90 days for security and debugging purposes.

**Session Data** includes information about your authenticated sessions, including session creation and expiration timestamps, and the actions you take within the Service.

**Device Information** includes information about the device you use to access the Service, including device type, operating system version, and browser configuration.

**Cookies and Similar Technologies** are described in detail in Section 9 of this Policy.

### 1.3 Information Collected from Third-Party Services

**Google Gmail API Data**: When you connect your Gmail account, InboxBrief accesses email metadata (sender, subject, snippet) from your Gmail inbox as described in InboxBrief's Google User Data Privacy Policy. InboxBrief does not access full email body content or attachments.

**Microsoft Outlook API Data**: When you connect your Outlook account, InboxBrief accesses email metadata (sender, subject, snippet) from your Outlook inbox. InboxBrief requests only the `Mail.Read` and `User.Read` Microsoft Graph API permissions.

**OAuth Profile Data**: When you authenticate using Google or Microsoft OAuth, InboxBrief receives your name, email address, and profile picture URL from the respective OAuth provider. Profile picture URLs are stored for display purposes within the Service.

---

## Section 2 — How We Use Your Information

InboxBrief uses your personal information for the following purposes:

### 2.1 Service Delivery

The primary purpose for which InboxBrief processes your personal data is to deliver the email briefing service you have requested. This includes fetching emails from your connected email accounts, classifying emails using AI, generating natural-language SMS briefings, and delivering those briefings to your registered phone number via Twilio.

### 2.2 Account Management

InboxBrief uses your personal data to create and manage your account, verify your identity, process payments, manage your subscription, and provide customer support.

### 2.3 Service Improvement

InboxBrief uses aggregated and anonymized usage data to improve the Service, including improving AI classification accuracy, optimizing briefing delivery timing, and developing new features. InboxBrief does not use your individual email content to train AI models.

### 2.4 Communications

InboxBrief uses your email address to send transactional communications related to your account, including account verification emails, subscription receipts, payment failure notifications, security alerts, and service announcements. InboxBrief may also send marketing communications to users who have opted in to receive them. You may opt out of marketing communications at any time by clicking the unsubscribe link in any marketing email or by contacting support@inboxbrief.com.

### 2.5 Legal Compliance and Security

InboxBrief uses your personal data as necessary to comply with applicable laws and regulations, to respond to legal process, to protect the rights and safety of InboxBrief and its users, and to detect, prevent, and investigate fraud, security incidents, and other harmful activities.

---

## Section 3 — Third-Party Service Providers and Data Processors

InboxBrief shares your personal data with the following categories of third-party service providers who process data on InboxBrief's behalf:

### 3.1 Google LLC (Gmail API and OAuth)

**Role**: Data Processor (for Gmail API access); Identity Provider (for Google OAuth authentication) **Data Shared**: OAuth tokens (access and refresh); email metadata (sender, subject, snippet) processed via Gmail API **Purpose**: Email inbox access for briefing generation; user authentication **Data Location**: United States (Google's infrastructure) **Privacy Policy**: https://policies.google.com/privacy **Applicable Terms**:

Google API Services User Data Policy (https://developers.google.com/terms/api-services-user-data-policy)

InboxBrief's use of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. InboxBrief uses Google user data only to provide the email briefing service, does not use Google user data for advertising, and does not allow human access to Google user data except as required for security investigations or legal compliance.

### 3.2 Microsoft Corporation (Outlook API and OAuth)

**Role**: Data Processor (for Outlook API access); Identity Provider (for Microsoft OAuth authentication) **Data Shared**: OAuth tokens (access and refresh); email metadata (sender, subject, snippet) processed via Microsoft Graph API **Purpose**: Email inbox access for briefing generation; user authentication **Data Location**: United States (Microsoft's infrastructure) **Privacy Policy**: https://privacy.microsoft.com/en-us/privacystatement **Applicable Terms**: Microsoft API Terms of Use (https://learn.microsoft.com/en-us/legal/microsoft-apis/terms-of-use)

InboxBrief requests only the minimum Microsoft Graph API permissions necessary to deliver the Service (`Mail.Read` and `User.Read`). Microsoft OAuth tokens are stored in AES-256-GCM encrypted form and are never transmitted in plaintext.

### 3.3 Twilio, Inc. (SMS Delivery)

**Role**: Data Processor **Data Shared**: Your registered phone number (E.164 format); AI-generated briefing text (does not contain raw email content) **Purpose**: SMS delivery of your email briefings **Data Location**: United States (Twilio's infrastructure) **Privacy Policy**: https://www.twilio.com/en-us/legal/privacy **Applicable Terms**: Twilio Terms of Service (https://www.twilio.com/en-us/legal/tos); Twilio Messaging Policy (https://www.twilio.com/en-us/legal/messaging-policy)

InboxBrief does not share your email content, OAuth tokens, or account credentials with Twilio. Twilio receives only your phone number and the generated briefing text for delivery purposes. InboxBrief maintains required A2P 10DLC registration for commercial SMS delivery in the United States.

### 3.4 Stripe, Inc. (Payment Processing)

**Role**: Data Processor and Independent Data Controller (for payment data) **Data Shared**: Your name, email address, and payment information (collected directly by Stripe); Stripe Customer ID and Subscription ID (stored by InboxBrief) **Purpose**: Payment processing, subscription management, fraud prevention **Data Location**: United States (Stripe's infrastructure) **Privacy Policy**: https://stripe.com/privacy **Applicable Terms**: Stripe Services Agreement (https://stripe.com/legal/ssa)

Stripe is certified as a PCI DSS Level 1 Service Provider. InboxBrief does not store your payment card numbers, CVV codes, or bank account information. Stripe may independently process your personal data as a data controller for fraud prevention and compliance purposes; such processing is governed by Stripe's Privacy Policy.

### 3.5 OpenRouter, Inc. (AI Processing)

**Role**: Data Processor **Data Shared**: Email metadata (sender name, subject line, email snippet up to 300 characters) for AI classification and briefing generation **Purpose**: AI-powered email classification and natural-language briefing generation **Data Location**: United States (OpenRouter's infrastructure) **Privacy Policy**: https://openrouter.ai/privacy **Applicable Terms**: OpenRouter Terms of Service (https://openrouter.ai/terms)

InboxBrief has configured its OpenRouter integration to use AI models that do not use submitted data for model training by default. Email metadata submitted to OpenRouter is used solely to generate your briefing and is not retained by OpenRouter after the API call completes. InboxBrief does not transmit full email body content or attachments to OpenRouter.

### 3.6 PingCAP, Inc. (Database Infrastructure — TiDB Cloud)

**Role**: Data Processor **Data Shared**: All data stored in InboxBrief's database, including encrypted OAuth tokens, encrypted briefing summaries, account information, and subscription data **Purpose**: Database hosting and management **Data Location**: United States **Privacy Policy**: https://pingcap.com/privacy-policy/

All data stored in TiDB Cloud is encrypted at rest. PingCAP does not have access to InboxBrief's encryption keys and cannot decrypt stored tokens or briefing content.

---

## Section 4 — Data Retention

InboxBrief retains your personal data for the periods described in the following table. After the applicable retention period, data is permanently deleted from InboxBrief's systems unless retention is required by applicable law.

| Data Category | Retention Period | Deletion Trigger |
|---|---|---|
| Account registration data | Duration of account + 30 days | Account deletion |
| Google OAuth tokens | Until revoked or account deletion | Account deletion or manual disconnect |
| Microsoft OAuth tokens | Until revoked or account deletion | Account deletion or manual disconnect |
| Encrypted briefing summaries | 90 days | Account deletion or user request |
| Briefing logs (metadata only) | 12 months | Account deletion |
| Phone number (encrypted) | Duration of account | Account deletion |
| Payment records (Stripe IDs only) | 7 years | Required for tax/accounting compliance |
| Audit logs | 12 months | Automatic purge |
| Support communications | 3 years | Account deletion or user request |
| Session cookies | 30 days of inactivity | Session expiry or logout |
| Server log data | 90 days | Automatic purge |

---

## Section 5 — International Data Transfers

InboxBrief's primary server infrastructure is located in the United States. If you are accessing the Service from outside the United States, your personal data will be

transferred to, stored in, and processed in the United States. The United States may not provide the same level of data protection as your home country.

For users in the European Economic Area (EEA), United Kingdom, or Switzerland, InboxBrief relies on the following legal bases for transferring personal data to the United States: (a) Standard Contractual Clauses (SCCs) adopted by the European Commission; (b) your explicit consent, provided when you create an account and connect your email accounts; and © the necessity of the transfer for the performance of the contract between you and InboxBrief.

InboxBrief's third-party service providers (Google, Microsoft, Twilio, Stripe, OpenRouter) may also process your data in the United States or other jurisdictions. Each provider maintains its own international data transfer mechanisms, including SCCs and Privacy Shield successor frameworks where applicable.

---

## Section 6 — Your Privacy Rights

### 6.1 Rights Available to All Users

Regardless of your location, InboxBrief provides the following rights with respect to your personal data:

**Right to Access**: You may request a copy of all personal data InboxBrief holds about you. InboxBrief will provide a machine-readable export within 30 days of receiving your request.

**Right to Correction**: You may request correction of inaccurate or incomplete personal data. InboxBrief will review and correct inaccurate data within 15 business days.

**Right to Deletion**: You may request deletion of your personal data. InboxBrief will delete your data within 30 days, subject to retention requirements described in Section 4.

**Right to Portability**: You may request your personal data in a portable, machine-readable format.

**Right to Opt Out of Marketing**: You may opt out of marketing communications at any time by clicking the unsubscribe link in any marketing email or by contacting

support@inboxbrief.com.

## 6.2 California Consumer Privacy Act (CCPA) Rights

California residents have the following additional rights under the CCPA:

**Right to Know**: You have the right to know what personal information InboxBrief collects, uses, discloses, and sells about you.

**Right to Delete**: You have the right to request deletion of your personal information, subject to certain exceptions.

**Right to Opt Out of Sale**: InboxBrief does not sell your personal information. If InboxBrief ever engages in the sale of personal information, California residents will have the right to opt out.

**Right to Non-Discrimination**: InboxBrief will not discriminate against you for exercising your CCPA rights.

**Shine the Light**: California residents may request information about disclosures of personal information to third parties for their direct marketing purposes. InboxBrief does not disclose personal information to third parties for direct marketing purposes.

To exercise your CCPA rights, contact InboxBrief at support@inboxbrief.com with the subject line “CCPA Request.”

## 6.3 General Data Protection Regulation (GDPR) Rights

Users in the European Economic Area, United Kingdom, and Switzerland have the following additional rights under the GDPR:

**Right to Restriction of Processing**: You may request that InboxBrief restrict processing of your personal data in certain circumstances.

**Right to Object**: You may object to InboxBrief’s processing of your personal data based on legitimate interests.

**Right to Lodge a Complaint**: You have the right to lodge a complaint with your local data protection authority if you believe InboxBrief has violated your privacy rights.

**Legal Bases for Processing**: InboxBrief processes your personal data on the following legal bases: (a) performance of a contract — processing necessary to deliver the Service; (b) legitimate interests — processing necessary for InboxBrief's legitimate business interests, including security, fraud prevention, and service improvement; © legal obligation — processing required by applicable law; and (d) consent — processing for which you have provided explicit consent, including marketing communications and Google/Microsoft OAuth access.

To exercise your GDPR rights, contact InboxBrief at support@inboxbrief.com with the subject line "GDPR Request."

---

## Section 7 — Security

### 7.1 Technical Safeguards

InboxBrief implements the following technical safeguards to protect your personal data:

All OAuth tokens (Google and Microsoft) are encrypted using AES-256-GCM encryption with a randomly generated initialization vector (IV) per encryption operation before being stored in the database. Briefing summaries are also stored in AES-256-GCM encrypted form. All data in transit between your browser and InboxBrief's servers is protected by TLS 1.2 or higher. Database connections use encrypted SSL/TLS connections. InboxBrief's servers are protected by network firewalls, intrusion detection systems, and regular security patching.

### 7.2 Organizational Safeguards

Access to InboxBrief's production database is restricted to authorized server processes only. No InboxBrief employee has routine access to user OAuth tokens, email content, or briefing summaries. Administrative database access requires multi-factor authentication and is logged for audit purposes. InboxBrief conducts periodic security reviews of its data handling infrastructure.

### 7.3 Incident Response

In the event of a security incident that may have resulted in unauthorized access to your personal data, InboxBrief will notify you within 72 hours of discovering the incident, consistent with applicable breach notification laws. InboxBrief will also notify relevant data protection authorities as required by applicable law.

### 7.4 No Absolute Security

No security system is impenetrable. InboxBrief cannot guarantee the absolute security of your personal data. In the event of a security breach, InboxBrief will take all reasonable steps to minimize the impact and to notify affected users as required by law.

---

## Section 8 — Children's Privacy

The Service is not directed to children under the age of 13 (or 16 in the EEA). InboxBrief does not knowingly collect personal information from children under 13. If InboxBrief becomes aware that it has collected personal information from a child under 13 without verifiable parental consent, it will take steps to delete that information as quickly as possible. If you believe that a child under 13 has provided personal information to InboxBrief, please contact support@inboxbrief.com.

---

## Section 9 — Cookies and Tracking Technologies

### 9.1 Types of Cookies Used

InboxBrief uses the following types of cookies and similar tracking technologies:

**Essential Cookies** are necessary for the Service to function and cannot be disabled. These include session cookies that maintain your authenticated state after login and security cookies that protect against cross-site request forgery (CSRF) attacks. Session cookies are HttpOnly, SameSite=None, and Secure, meaning they cannot be accessed by client-side JavaScript and are only transmitted over encrypted HTTPS connections.

**Preference Cookies** store your preferences and settings, such as your chosen language and briefing schedule. These cookies are stored in your browser's local storage and persist until you clear your browser data.

**Analytics Cookies**, if used, collect anonymized information about how users interact with the Service to help InboxBrief improve the user experience. InboxBrief will provide notice and obtain consent before deploying analytics cookies.

### 9.2 Cookie Management

You may control cookies through your browser settings. Most browsers allow you to block or delete cookies. However, blocking essential cookies may prevent you from using certain features of the Service. For more information about managing cookies, visit https://www.allaboutcookies.org.

### 9.3 Do Not Track

InboxBrief does not currently respond to "Do Not Track" signals from browsers, as there is no industry-standard interpretation of such signals. InboxBrief will update this Policy if it adopts a Do Not Track policy.

---

## Section 10 — Third-Party Links and Services

The Service may contain links to third-party websites, applications, and services. InboxBrief is not responsible for the privacy practices of third-party services and encourages you to review the privacy policies of any third-party service you access through the Service. The inclusion of a link to a third-party service does not constitute InboxBrief's endorsement of that service.

---

## Section 11 — Business Transfers

If InboxBrief is involved in a merger, acquisition, reorganization, bankruptcy, or sale of all or a portion of its assets, your personal data may be transferred as part of that transaction. InboxBrief will provide notice before your personal data is transferred and becomes subject to a different privacy policy. If the acquiring entity's privacy practices

are materially different from those described in this Policy, InboxBrief will provide you with the opportunity to opt out of the transfer.

---

## Section 12 — Changes to This Policy

InboxBrief reserves the right to modify this Privacy Policy at any time. We will provide notice of material changes by: (a) posting the updated Policy on this page with a revised "Last Reviewed" date; (b) sending an email notification to your registered email address at least 14 days before the changes take effect; and © displaying a prominent notice within the InboxBrief dashboard. Your continued use of the Service after the effective date of any changes constitutes your acceptance of the revised Policy.

---

## Section 13 — Contact Information and Data Protection Officer

For questions, concerns, or requests related to this Privacy Policy or InboxBrief's data practices, please contact:

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

For urgent privacy matters, please use the subject line "PRIVACY URGENT" in your email communication. InboxBrief will respond to all privacy inquiries within 5 business days.

---

## Section 14 — Definitions

For the purposes of this Privacy Policy, the following terms have the meanings set forth below:

**"Personal Data"** means any information that identifies or could reasonably identify a natural person, including name, email address, phone number, IP address, and device identifiers.

**“Processing”** means any operation performed on personal data, including collection, storage, retrieval, use, disclosure, transmission, and deletion.

**“Data Controller”** means the entity that determines the purposes and means of processing personal data. InboxBrief is the data controller for personal data processed through the Service.

**“Data Processor”** means an entity that processes personal data on behalf of a data controller. InboxBrief’s third-party service providers (Google, Microsoft, Twilio, Stripe, OpenRouter, PingCAP) are data processors with respect to data processed on InboxBrief’s behalf.

**“Sensitive Personal Data”** means personal data that requires heightened protection, including health information, financial information, government identification numbers, and biometric data. InboxBrief does not intentionally collect sensitive personal data.

---

*This Privacy Policy was last reviewed and updated on March 21, 2026. InboxBrief is committed to maintaining transparent data practices and to protecting the privacy of all users of its Service.*