Cambrient AI, Inc – Privacy Policy

Effective Date: July 8, 2025

Cambrient AI, Inc ("**Cambrient AI**," "**we,**" "**our,**" or "**us**") provides a cloud-based email-security service that connects to Microsoft 365 via the Microsoft Graph API to identify, quarantine, and label suspected phishing emails (the "**Service**").
This Privacy Policy explains how we collect, use, disclose, and secure personal information when customers and end-users ("**you**") access or use the Service, visit our websites, or otherwise interact with us.

> **Note:** This template is for general informational purposes only. Consult legal counsel to ensure it meets your specific obligations.

---

1. Information We Collect

Category	Examples	Source
Account Information	Company name, admin name, business email, billing address, subscription tier	Provided by the customer administrator during sign-up
Email Data	Header, body, attachments, metadata, sender and recipient addresses of messages flagged as suspicious	Pulled via Microsoft Graph API after the customer grants permissions
Diagnostic & Log Data	IP address, browser/OS type, API request IDs, timestamps, error logs	Collected automatically when you interact with the Service
Support Communications	Issue descriptions, screenshots, contact details	Provided voluntarily when you contact support

We do **not** intentionally collect special categories of personal data (e.g., health or biometric data) nor data from children under 16.

---

2. How We Use Information

Purpose	Legal Basis (GDPR)

Provide, secure, and maintain the Service (identify phishing, store flagged messages, deliver dashboards)	**Performance of a contract**
Troubleshoot, analyze usage, and improve features and accuracy	**Legitimate interests**
Send administrative or security notifications (e.g., incident alerts, policy updates)	**Performance of a contract / Legitimate interests**
Process payments and manage subscriptions	**Performance of a contract / Legal obligation**
Comply with legal requests and enforce our Terms of Use	**Legal obligation / Legitimate interests**

Cambrient AI does **not** sell or rent your personal information.

---

3. Sharing & Disclosure

We share personal information only:

1. **Within Cambrient AI, Inc** on a need-to-know basis under strict access controls.
2. **With sub-processors** that help us run the Service (e.g., cloud hosting, email delivery, analytics), bound by written data-processing agreements. A current list is available upon request.
3. **For legal reasons** if required by law, subpoena, or to protect the rights, property, or safety of Cambrient AI, our customers, or the public.
4. **With your consent** or at your direction (e.g., exporting flagged-mail reports to a third-party ticketing system you configure).

---

4. Data Retention

- **Flagged Email Data**: Retained **30 days** by default, then automatically and permanently deleted, unless the customer specifies a shorter or longer retention period in their admin settings.

- **Account & Billing Data**: Retained for the life of the subscription and as long as necessary to satisfy legal or accounting requirements (typically up to 7 years).
- **Diagnostic Logs**: Retained no longer than **12 months**.

After the relevant retention period elapses—or upon verified deletion request—data is securely erased from backups and active systems.

---

5. Security Measures

We employ industry-standard safeguards, including:

- AES-256 encryption at rest and TLS 1.2+ in transit
- Network firewalls, intrusion detection, and automated malware scanning
- Multi-factor authentication for administrative access and code repositories
- Regular vulnerability scanning and annual penetration testing
- Strict access controls based on the principle of least privilege

No security measure is perfect, but we continually improve our defenses.

---

6. International Transfers

Cambrient AI, Inc is headquartered in the United States. We may transfer and process information in the U.S. and other countries where we or our sub-processors operate.
When we transfer personal data from the European Economic Area (EEA), United Kingdom, or Switzerland to countries without an adequacy decision, we rely on lawful transfer mechanisms such as the EU Standard Contractual Clauses.

---

7. Your Rights

Depending on your location, you may have rights to:

- Access, correct, or delete your personal information
- Restrict or object to certain processing
- Receive a portable copy of your data
- Withdraw consent at any time (where processing is based on consent)
- Lodge a complaint with a supervisory authority

Customers can exercise these rights through their admin portal or by emailing **no-reply@cambrient.ai**. We will verify and respond within the timeframes required by law.

---

8. Cookies & Similar Technologies

Our public websites use cookies for essential functionality and aggregated analytics (e.g., page-load performance). We do not use advertising or tracking cookies in the Service dashboard itself. You can manage cookie preferences in your browser.

---

9. Children's Privacy

The Service is directed to businesses and not to children. We do not knowingly collect personal data from anyone under 16. If you believe we have collected such data inadvertently, contact us at **no-reply@cambrient.ai** so we can delete it.

---

10. Changes to This Policy

We may update this Privacy Policy periodically. If we make material changes, we will notify you via the Service or email and update the "Effective Date." Your continued use of the Service after the changes become effective constitutes acceptance.

---

11. Contact Us

Cambrient AI, Inc
11549 Tralee Dr, Great Falls, VA 22066 USA
Email: **no-reply@cambrient.ai**

By using the Service, you acknowledge that you have read and understood this Privacy Policy.