

Privaseer Privacy Policy

Last updated: July 23, 2026

Privaseer is committed to protecting your privacy. This policy explains exactly what data we collect, how we handle it, where it is stored, and our strict policies against sharing it.

1. Data Collection

We minimize data collection by design. We collect only the following information necessary for the extension to function:

Installation ID: A random identifier generated on your device when you install Privaseer. It is completely anonymous and not linked to your name, Google account, or real-world identity.

Website Domain Information: When Privaseer analyzes a cookie-consent banner or blocks a tracker, the domain of the site (e.g., "example.com") is processed to determine privacy risks.

Cookie-Consent Analysis Results: The type of consent tool detected, the presence of a "reject" option, and a confidence score are collected to record consent activity and improve detection accuracy. We do not collect or read your actual cookie values.

Burner Email Addresses & Forwarding: The disposable email aliases generated by the extension are collected and stored so they remain available across your browsing sessions. If you choose to set a personal forwarding email address in Settings, that address is also stored so mail sent to your burner alias can be routed to your real inbox. When a burner alias receives an email, its subject and body are processed on our backend to strip tracking pixels and tracking links before the message is forwarded to you.

Locally-Stored Data: Your settings, your cached privacy score, and your blocked-tracker history are collected and stored strictly locally within your browser (chrome.storage.local).

Optional Telemetry & Feedback: If you explicitly choose to submit feedback or enable telemetry in Settings, anonymized usage events (e.g., how many trackers were blocked) are collected to monitor performance.

Detection Feedback: If you report an incorrect cookie-banner detection ("false positive"), the site's domain, the page URL, the patterns that were detected, and any optional comment you add are collected to help us improve detection accuracy.

What we DO NOT collect: We never collect passwords, payment information, health data, precise location, or a continuous stream of your browsing history.

2. Data Handling & Use

We handle your data strictly to provide and improve the Privaseer features you use:

Domain & Consent Data: Used to detect deceptive cookie banners and improve our scanner's accuracy over time.

Burner Emails & Forwarding: Used solely to generate, manage, and route disposable email aliases, including delivering sanitized mail to your real inbox when you've configured a forwarding address.

Detection Feedback: Used only to review and correct false-positive reports and improve scanning accuracy over time.

Locally-Stored Data: Handled entirely by your own browser to instantly calculate and display your Privacy Score without pinging external servers.

Telemetry & Feedback: Used only to diagnose software issues and monitor extension performance in aggregate. It is never used to build advertising profiles.

3. Data Storage & Retention

Local Storage: Your settings, privacy scores, and tracker histories are stored on your local device. This data remains on your device until you clear it or uninstall the extension.

Server-side Storage: Data required for cross-session functionality (like your generated burner aliases and anonymized consent analytics) is stored securely on our backend infrastructure (Supabase).

Retention: Server-side data is retained only for as long as necessary to provide the service. It is deleted when the associated burner alias is deleted, or when you explicitly request deletion by contacting us.

4. Data Sharing & Disclosure

Privaseer has a strict zero-selling policy.

No Selling: We do not sell, rent, or trade your data to any third parties.

No Advertising: We do not share your data with advertisers, nor do we use it for cross-site tracking, credit, or lending decisions.

Service Providers: We only share data with trusted backend infrastructure providers (e.g., database hosting) acting strictly as data processors on our behalf. They are legally bound to not use your data for their own purposes.

5. Security

Data sent between the extension and our backend is encrypted in transit using HTTPS/TLS. Access to stored data is restricted only to the systems necessary to provide the features described above.

6. Your Choices and Rights

Total Control: You can view, export, and permanently delete all locally-stored data from the extension's Settings page at any time.

Opt-in Features: Burner email generation and telemetry are completely optional and can be disabled at any time.

Right to Deletion: To request the permanent deletion of any data stored on our servers (including burner email records or telemetry tied to your installation ID), please email us at the address below and it will be removed immediately.

7. Children's Privacy

Privaseer is not directed at children under 13, and we do not knowingly collect data from children.

8. Changes to This Policy

If we make material changes to this policy, we will update the "Last updated" date above and, where required, notify users through the extension.

9. Contact Us

For any privacy questions, concerns, or data deletion requests, contact us at:
privaseer.hostinger@gmail.com