Privacy Policy

Last update: May 15, 2025

1. Introduction

1.1. This Privacy Policy (“Policy”) explains how Secserv.me (“Secserv,” “we,” “us”) handles data in connection with your use of our end-to-end encrypted message platform at https://v2.secserv.me/ and https://appv2.secserv.me/. Free messages are encrypted/decrypted entirely client-side without any Web3 interaction; paid messages utilize Web3 only for on-chain payment.

1.2. We do not collect or store any personal data. The only information ever held by Secserv is the encrypted payloads you provide when uploading messages or files.

2. Data We Handle

2.1. Encrypted Payloads: Client-side AES-256 blobs containing any combination of text and file data you upload.

2.2. Zero Collection of PII or Tracking Data

- We do not collect names, emails, phone numbers, IP addresses, device fingerprints, location, or analytics cookies.
- We do not log or process EXIF data, file metadata, or headers—such information remains encrypted with your file and is never extracted or stored in plain form.

3. Purpose & Legal Basis

3.1. Deliver Messages: to decrypt and display your encrypted payload when you or a recipient access a link.

3.2. Enforce Settings: to apply TTL, delete-after-read, and other flags you configure.

3.3. Facilitate Payments: to trigger on-chain USDC payment workflows for paid messages.

All processing is initiated by your direct actions (uploading, setting options, or paying) and is strictly limited to these purposes.

4. Data Retention & Deletion

4.1. Encrypted payloads exist only until your chosen TTL expires or until first read (if delete-after-read was enabled).

4.2. After deletion, residual encrypted blobs are purged from storage within 24 hours.

4.3. No long-term user profiles or tracking records are maintained.

5. Security Measures

5.1. Client-Side Encryption: AES-256; decryption keys never leave your browser.

5.2. Transport Security: TLS 1.3 with HSTS for all network traffic.

5.3. Storage Security: Secserv holds no decryption keys and cannot view your content.

6. Your Rights & Anonymity

6.1. Because we do not hold any personal data, there is no PII to access, correct, or delete.

6.2. You may delete any remaining encrypted blobs via your removal link prior to first read.

6.3. If you require confirmation of deletion, use the same removal link URL you received upon message creation.

7. Third-Party Integrations

7.1. Wallet Providers & On-Chain Contracts

- We integrate with non-custodial wallet providers (e.g., MetaMask, WalletConnect) only to request transaction signatures. We never share any personal data with them, and they adhere to their own privacy policies.
- All payments execute via USDC smart contracts on the blockchain; these contracts process on-chain transfers and do not collect or store any off-chain personal information.

7.2. No off-chain KYC or personal data exchange occurs with any third party.

8. Updates to Policy

8.1. We may amend this Policy; new versions take effect upon posting at https://v2.secserv.me/ or https://appv2.secserv.me/

8.2. Continued use of the Platform implies acceptance of the updated Policy.

9. Contact

Data inquiries or concerns: ssgsystems@protonmail.com

Prepared May 15, 2025 • Secserv