

PRIVACY POLICY

Last Updated: February 16, 2025

This Privacy Policy describes how Envoid Shield Limited ("Company," "We," "Us," or "Our") collects, uses, and protects personal data when you access and use Envoid Services ("Service"). This policy applies to the Envoid mobile application ("App"), the Enport device ("Device"), and the web-based interface ("Web UI").

By using the Service, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with any part of this policy, you should refrain from using the Service.

1. Definitions

- **Account:** A unique profile created to access the Service or specific features.
- **Company:** Envoid Shield Limited, a Cyprus-registered entity (Registration Number HE 466493), with its principal office at 3 Griva Digeni Street, PATSALOS HOUSE, Floor 5, Office 501, 6030, Larnaca, Cyprus.
- **Consumer:** Any business, organization, or individual with an active Envoid Services license.
- **Cookies:** Small text files stored on your device to track browsing behavior and preferences.
- **Device (Enport):** The hardware component that processes and stores security analysis results within user premises.
- **Personal Data:** Any information that can identify an individual, either alone or combined with other details.
- **Service:** The cybersecurity services provided by Envoid Shield Limited, including the Enport device, the mobile application, and the web UI.
- **Usage Data:** Data automatically collected regarding Service interaction, including IP addresses, browser types, and session details.
- **Website:** The official website of Envoid, available at <https://www.envoid.com/> or other Company-managed domains.
- **You:** Any individual or entity accessing or using the Service, either personally or as a representative of an organization.

2. Data Collection and Use

2.1 Data Collected

By the Mobile App:

- The App itself **does not collect or store** personal data or system logs.
- The App communicates with the Enport device to:
 - Initiate security scans.
 - Retrieve analysis results containing security findings.
 - Provide links to reports stored on the Enport device or the client's self-hosted servers.
 - Display security recommendations.
- The App does not process, store, or transmit personal data outside the user's environment.

By the Enport Device:

- The Enport device collects and processes system logs from iOS devices for security analysis.
- These logs may contain personal data, including device identifiers, IP addresses, and metadata from installed applications.
- Data is stored locally on the Enport device or on a self-hosted server owned by the user.
- If the user opts for VPN-based cloud storage, data may be transmitted to a client-owned cloud server.

By the Web UI:

- The Web UI provides administrators access to security events, logs, and system configurations.
- It does not collect personal data unless the user explicitly provides it for support purposes.

3. Tracking Technologies & Cookies

The App does not use tracking technologies, cookies, or analytics tools. The Website may use cookies to store user preferences and enhance functionality. Users can modify browser settings to disable cookies.

4. Data Storage and Security

- **No Cloud Storage by Default:** Envoid does not store customer data on its own servers.
- **Self-Hosted Model:** Data is stored within the user's own environment, either on the Enport device or on a self-hosted server.
- **Cloud Storage (Optional):** If the client chooses to use VPN cloud storage, data is hosted on a client-managed server.
- **Security Measures:** We implement industry-standard security measures to prevent unauthorized access or data loss. However, absolute security cannot be guaranteed.

5. Sharing of Data

Envoid does not share personal data with third parties, except in the following cases:

- **User's Choice:** If the user configures email or WhatsApp alerts, data may be transmitted through those selected channels.
- **Legal Compliance:** If required by law, we may disclose personal data to authorities.

6. App Store Compliance (Apple Requirements)

- **App Tracking Transparency (ATT):** The App does not track users across other apps or websites. No ATT request is required.
- **Data Linked to Users:** The App itself does not collect data; all processing occurs within the user-controlled Enport device.
- **Data Sharing:** No data is shared with third-party analytics or advertisers.

7. User Rights and Consent

7.1 Consent

- By using the App and pairing it with the Enport device, the user consents to security scanning.
- If required, explicit consent mechanisms will be implemented.

7.2 User Rights (GDPR & CCPA Compliance)

Users in the EU (GDPR) and California (CCPA) have the right to:

- Access their data.
- Request corrections or deletion of personal data.
- Restrict processing or object to data use.
- Request data portability.
- File complaints with data protection authorities.

To exercise these rights, contact us at info@envoio.com.

8. Retention of Data

- **Mobile App:** No data retention.
- **Enport Device:** Data is stored locally and managed by the user.
- **Web UI:** Data is stored only if the user provides it for support requests.

9. Changes to This Privacy Policy

We may update this Privacy Policy periodically. Updates will be posted on our Website, and users will be notified of significant changes. The "Last Updated" date at the top reflects the latest revision.

10. Contact Us

For any questions regarding this Privacy Policy, you can contact us at:

Email: info@envoio.com