RIMARI SENTINEL Global Privacy & Data Sovereignty Policy

Effective Date: January 3, 2026

Version: 2.1.0-PRIV

1. Data Collection & Processing Sovereignty

RIMARI Sentinel is engineered with a **"Local-First, Privacy-by-Design"** architecture.

- **Client-Side Processing**: The majority of scan data processing, visualization, and report generation (PDF/TXT) occurs entirely within the user's browser session.
- **Zero-Persistence Logging**: Kush-Tech Solutions does not maintain server-side logs of target URLs, specific scan results, or vulnerability findings.

2. Technical Information Probes

To provide infrastructure intelligence, the system performs targeted technical queries:

- **DNS & IP Lookups**: The scanner queries public DNS-over-HTTPS records and IP geolocation databases (ipinfo.io) to identify network providers and hosting locations.
- **Anonymity**: These technical probes do not transmit personally identifiable information (PII). No user tracking, marketing cookies, or third-party analytics are utilized within the platform.

3. Security Hardening & Obfuscation

To protect the integrity of the audit process and proprietary scanning logic, RIMARI Sentinel implements advanced security controls:

- **Anti-Inspection Layers**: The platform utilizes source code obfuscation and active detection to block unauthorized access to Developer Tools (F12, Ctrl+Shift+I).
- **Debugger Traps**: Built-in anti-analysis loops hinder unauthorized reverse-engineering attempts.

4. Compliance and Legal Responsibility

- **User Authorization**: RIMARI Sentinel is a tool for professional security research and authorized testing. Users are solely responsible for ensuring they have explicit, written permission to scan any target domain.
- **Jurisdiction**: This policy is governed by the data protection standards of the year 2026, prioritizing user anonymity and data sovereignty in alignment with global cybersecurity best practices.

Kush-Tech Solutions
Research-led AI Engineering and IT Solutions
https://kushtechsolutions.org