WHITELINT GLOBAL PRIVACY POLICY 2024

Effective from: April 2024

This Privacy Policy outlines how WhiteLint Global Pvt Ltd collects, uses, maintains, and discloses information obtained from users of the "WAFER" framework-based products ("Products"). As a provider of advanced network security solutions, we are deeply committed to ensuring the security and privacy of our users' information. We understand the critical interdependence between security and privacy and prioritize both aspects in all our operations and interactions.

By using our Products, users consent to the terms outlined in this Privacy Policy.

1. Information Collection:

a. Personal Information: We may collect personal identification information from users when they interact with our Products, including but not limited to when they set up or configure the device, register the device for updates or support, or engage with our Products through user interfaces. Users may be asked for, as appropriate, name, email address, and contact details. We will collect personal identification information from users only if they voluntarily submit such information to us.

b. Non-personal Information: We may collect non-personal information about users whenever they interact with our Products. This may include information related to device identifiers, such as IP addresses, model, firmware versions, operating system, time zone, MAC addresses, and other technical details about computing systems, Network Logs, filenames, and file paths. This information is not correlated with any personal information.

2. Use of the Collected Information:

We may use the collected information for the following purposes:

a) **Providing the WhiteLint Services:** This includes tasks such as offering maintenance and technical support, delivering product upgrades, addressing security and business continuity issues, and analysing and enhancing the WhiteLint Services. This also encompasses responding to new threats and developing new features to continually improve our offerings.
b) **Enforcement of Legal Terms:** We may use the collected information to enforce the legal terms that govern the WhiteLint Services.
c) **Compliance with Law and Protection of Rights, Safety, and Property:** We may use the information to comply with applicable laws and regulations and to protect the rights, safety, and property of individuals.
d) **Cyber security Research**: We may use the data for the purpose of cybersecurity research, aimed at identifying emerging threats, improving threat detection capabilities, and enhancing overall cybersecurity posture.
e) **Other Business Purposes:** We may use the information for other purposes requested or permitted by our customers or users, or as reasonably required to perform our business operations effectively.

Many WhiteLint Services leverage automated technology to identify and mitigate cybersecurity risks, such as by blocking or quarantining suspected malicious data. To enhance the security of our customers and aid them in their security compliance efforts, some WhiteLint Services utilize external threat information gathered in these scenarios to

bolster security for other customers facing similar threats. For example, if certain WhiteLint services detect a hacker attacking some of our customers, we may use information about that threat to help safeguard other customers from similar attacks. This proactive approach ensures that our customers' data receives enhanced protection, leveraging insights gained from past experiences.

3. Information Sharing Practices

For the purposes mentioned in Clause 2, we may share information with:
Our affiliates.

a) Our customers.
b) Third parties that assist us, such as resellers, marketing providers, testing providers, analytics providers, and providers of technical services (e.g., data storage and data backup).
c) Joint marketing partners.
d) Cyber security researchers (In House R&D Team).
e) Computer Emergency Response Teams (CERT).
f) Employers and others seeking verification of an individual's claimed certification status.
g) Entities involved in dispute resolution, such as arbitrators or opposing parties.
h) Entities involved in potential or actual significant corporate transactions or events.
i) Governmental entities.

4. Data Security:

We are dedicated to ensuring the utmost security of user data processed by the WAFER device. Our measures include physical, electronic and managerial procedures. These measures collectively safeguard against unauthorized access, alteration, disclosure, or destruction of personal information.

5. Information Sharing Practices

We maintain stringent confidentiality standards and refrain from selling, trading, or renting users' personal identification information to third parties. Although personal identification information is not shared, our use and disclosure of aggregated or de-identified data, which lacks personal identifiers, is not bound by the limitations outlined in this Privacy Policy. Such data may be disclosed to third parties without constraints for any purpose.

6. Security

We have implemented security measures in line with global information standards to safeguard your personal data, ensuring a level of protection that meets European Union standards, including those set forth in the General Data Protection Regulation (GDPR). Our efforts are directed towards protecting both personal data and network integrity, with a focus on enhancing network and information security.

7. Rights of Data Subjects

In alignment with the provisions of the GDPR, individuals identified as Data Subjects retain various rights concerning their personal data. These rights encompass the entitlement to access their data, rectify inaccuracies, request erasure, and avoid individual decision-making processes. Additionally, Data Subjects have the right to restrict the

processing of their personal data and avail themselves of data portability. To exercise these rights, individuals may submit a dated and signed written request to WhiteLint Global.

8. Legal Compliance

We are dedicated to adhering to all pertinent laws and regulations governing the collection, processing, and disclosure of personal information in India, including but not limited to the Information Technology Act, 2000 and the rules framed thereunder, and other relevant data protection legislation enacted by the Government of India.

9. Data Retention

We retain user data only for the period necessary to fulfil the purposes outlined in this Privacy Policy or as required by law. Once the retention period expires, we securely delete or anonymize the data in accordance with our data retention policies.

10. Changes to This Privacy Policy

We reserve the right to update or modify this Privacy Policy at any time. Users are encouraged to check our web page periodically for any changes. By continuing to use our products and services after any modifications to this policy, users acknowledge and agree to the updated terms.

11. Contact Us:

If you have any questions or concerns regarding this Privacy Policy or the privacy practices related to our products and services, please contact us at contact@whitelint.com.