HACKTAPE TECHNOLOGIES PRIVATE LIMITED
CIN: Incorporated under the Companies Act, 2013 (India) • Regulatory & Corporate Repository

PRIVACY POLICY & DATA PROTECTION

HACKTAPE TECHNOLOGIES PRIVATE LIMITED • Effective Date: November 12, 2026

1. INTRODUCTION AND SCOPE

Welcome to **Hacktape** (the "Platform"), owned, developed, and operated by **HACKTAPE TECHNOLOGIES PRIVATE LIMITED** ("Company", "we", "us", or "our"), a private limited company incorporated under the laws of India, having its principal office in India (contact email: `privacy@hacktape.io`).

This Privacy Policy ("Policy") sets forth our policies and procedures regarding the collection, storage, processing, transfer, protection, and disclosure of personal data and operational information when you access or interact with:

1. The Hacktape website located at `https://hacktape.io` (and its subdomains);
2. The browser-native interactive cyber range, challenge environments, and learning paths;
3. Our automated flag submission, leaderboard, and progression engines;
4. Our verifiable cryptographic certificate validation services; and
5. Associated billing, customer support, and community interfaces.

By accessing or using Hacktape, creating an account, redeeming an authorized access voucher, or purchasing a subscription, you acknowledge that you have read, understood, and agreed to the practices described in this Privacy Policy. If you do not agree with any part of this Policy, you must immediately terminate access to and use of our Platform.

2. ARCHITECTURAL PRIVACY: BROWSER-NATIVE $0-COMPUTE EXECUTION

A foundational tenet of Hacktape's technical architecture is our **browser-native, zero-server-compute execution paradigm**:

2.1 Client-Side WebAssembly (WASM) Sandbox

- Unlike conventional cloud-hosted cyber ranges that provision centralized server virtual machines (VMs) and record centralized interactive shell logs, Hacktape executes its core ephemeral Linux virtualization workloads **entirely within your client web browser** utilizing WebAssembly (WASM) emulation (including v86 / x86 CPU emulation).
- **No Keystroke Logging or Shell Interception:** The interactive terminal sessions, bash commands, exploit scripts, filesystem manipulations, and memory states generated within your local WASM sandbox execute directly in your browser's runtime environment. **Hacktape does not monitor, intercept, record, or store your interactive terminal keystrokes, standard input (stdin), standard output (stdout), or guest filesystem contents on our servers.**

- **Local Ephemerality:** When you terminate your browser session, reload the page, or destroy an exercise sandbox, the local memory and filesystem states are purged from your client browser memory, preserving your operational privacy.

2.2 Server-Side Interactions Limited to Progression Telemetry

The only data transmitted from your client sandbox to Hacktape's backend infrastructure consists of:

1. Proof-of-concept cryptographic flags submitted for automated objective validation;
2. Timestamps marking exercise launch, step completion, and milestone unlocking;
3. Platform telemetry metrics (e.g., emulator boot latency, WASM frame rates) strictly utilized to ensure operational stability and diagnose browser compatibility issues.

3. CATEGORIES OF INFORMATION WE COLLECT

We collect only the minimum personal information necessary to deliver, secure, and operate the Platform.

3.1 Information You Provide Directly

- **Account Registration Data:** When you register an account, we collect your email address, chosen handle / username, full name (optional for certificate generation), and hashed credentials.
- **Single Sign-On (SSO) and OAuth Authentication:** If you register or authenticate via third-party providers (such as GitHub OAuth or Google OAuth), we receive your verified email address, unique provider identifier, public display name, avatar URL, and OAuth authorization tokens via standard PKCE (Proof Key for Code Exchange) flows. We do not access or store your third-party account passwords or private repositories.
- **Profile and Identity Information:** Custom avatar preferences, public bio, social links (e.g., LinkedIn or GitHub profiles), and country of origin (used for regional leaderboard aggregation if opted in).
- **Payment and Billing Information:** When subscribing to Hacktape Pro (Monthly or Annual plans), billing data is collected directly by our PCI-DSS Level 1 compliant payment gateway partners (Stripe, Inc. and Razorpay Software Private Limited). We collect and retain only truncated transaction metadata, including transaction ID, card brand, last four digits of the payment instrument, billing postal code, invoice state, and subscription expiration date. **We never store, process, or transmit raw credit/debit card numbers or CVV codes on our servers.**
- **Promotional and Voucher Codes:** Alphanumeric redemption codes submitted to activate complimentary or promotional access (e.g., Crew or Launch Customer vouchers).
- **Support Communications:** Text, email inquiries, diagnostic logs, or bug reports submitted via our support desks (`support@hacktape.io` or `billing@hacktape.io`).

3.2 Information Collected Automatically

- **System Telemetry & Device Data:** Internet Protocol (IP) address, browser vendor and version, WebAssembly and WebGL feature availability, operating system, preferred language, and referring URLs.
- **Daily Salted IP Hashing:** To protect against abuse, brute-force attacks, and credential stuffing while prioritizing user anonymity, raw IP addresses associated with terminal connections and rate-limiting counters are converted using a cryptographic one-way hash combined with a daily rotating salt before persistent indexing.
- **Challenge Progress & Ranking Metrics:** Solved room IDs, verified flag timestamps, accumulated Experience Points (XP), streak counters, badge acquisitions, leaderboard standings, and issued certificate serial numbers.
- **Session Tokens & Cookies:** Minimal, strictly necessary cryptographic session identifiers stored in HTTP-only, secure, SameSite cookies to maintain authenticated operator state across requests.

4. LEGAL BASES FOR PROCESSING (GDPR & DPDP ACT 2023)

Under the European Union General Data Protection Regulation (Regulation (EU) 2016/679 - "GDPR"), the United Kingdom Data Protection Act 2018, and the Indian Digital Personal Data Protection Act, 2023 ("DPDP Act"), we process your personal data under the following lawful bases:

Purpose of Processing	Lawful Basis (GDPR / International)	Lawful Basis (DPDP Act 2023)
Account creation, authentication, and session management	Contractual Necessity (Art. 6(1)(b))	Performance of requested service / Specified purpose
Delivering interactive WASM lab environments and verifying flags	Contractual Necessity (Art. 6(1)(b))	Specified purpose consented to upon registration
Processing subscription payments and generating invoices	Contractual Necessity & Legal Obligation (Art. 6(1)(b), (c))	Compliance with applicable tax, financial, and accounting laws
Issuing tamper-proof Ed25519 cryptographic certificates	Contractual Necessity & Legitimate Interest (Art. 6(1)(b), (f))	Specified educational purpose
Preventing malicious attacks, DDoS, credential stuffing, and platform abuse	Legitimate Interests (Art. 6(1)(f))	Legitimate uses / Security of IT systems
Transactional communications, billing receipts, and security alerts	Contractual Necessity (Art. 6(1)(b))	Specified communication purpose
Marketing updates, release notes, and newsletters	Freely Given Consent (Art. 6(1)(a))	Express affirmative consent (opt-in)

5. HOW WE USE YOUR INFORMATION

We strictly limit the use of collected data to the following operational purposes:

1. **Platform Service Delivery:** Authenticating users, maintaining persistent learning progress, calculating streaks, awarding XP, and dynamically rendering challenge modules.
2. **Cryptographic Certificate Verification:** Storing public certificate records—including candidate legal name, track title, completion timestamp, and Ed25519 public key signature—allowing third-party employers and academic institutions to verify authentic credentials via `https://hacktape.io/verify`.
3. **Leaderboards and Competitive CTF:** Displaying operator handles, avatar graphics, rank, and XP metrics on public or private leaderboards (users may elect to remain pseudonymous).
4. **Platform Security and Integrity:** Enforcing strict rate limits, auditing anomalous flag submission velocity (anti-cheat detection), validating single-use voucher integrity, and thwarting unauthorized automated scrapers.
5. **Customer Support and Dispute Resolution:** Investigating platform defects, resolving subscription billing inquiries, and executing authorized refunds.

6. COOKIES AND LOCAL STORAGE DISCLOSURE

Hacktape employs a strictly utilitarian cookie and storage philosophy. We do not engage in cross-site behavioral advertising or third-party marketing trackers.

- **Strictly Necessary Cookies:** We deploy secure, `HttpOnly`, `SameSite=Lax` or `SameSite=Strict` cookies to securely maintain your authentication session token.
- **Client-Side Local Storage (IndexedDB / localStorage):** Utilized exclusively within your browser to cache WebAssembly binary images (`.wasm`), kernel rootfs assets, and ephemeral lab state to expedite load times and eliminate unnecessary network requests.

You may instruct your web browser to reject cookies; however, disabling essential session cookies will prevent you from authenticating and accessing authenticated cyber range features.

7. SHARING AND DISCLOSURE OF INFORMATION

We treat your personal data with utmost confidentiality. **Hacktape has never sold, rented, or commercialized your personal data to data brokers or third-party advertisers, and will never do so.**

We disclose personal data only under the following limited circumstances:

1. **Vetted Service Providers (Data Processors):** We share data with trusted infrastructure and payment partners bound by stringent Data Processing Agreements (DPAs) and confidentiality obligations:
   - **Cloud Infrastructure & Managed Database:** Neon, Inc. (PostgreSQL database hosting with encryption at rest and in transit).
   - **Hosting & Content Delivery:** Vercel Inc. and Cloudflare, Inc. (global edge routing, static asset caching, DDoS mitigation).
   - **Payment Gateways:** Stripe, Inc. and Razorpay Software Private Limited (secure checkout, tax compliance, recurring billing).
   - **Transactional Email Services:** Resend / Amazon SES (system notifications, password resets, verification links).
2. **Public Leaderboard and Certificates:** If you participate in public rooms or earn completion certificates, your chosen username, rank, XP, and public certificate metadata are publicly visible. You may configure your profile privacy settings at any time.
3. **Legal Compliance and Enforceable Government Requests:** We may disclose records if required by a valid court order, subpoena, warrant, or binding statutory mandate under Indian law or applicable foreign jurisdictional treaties.
4. **Protection of Vital Rights:** When reasonably necessary to investigate violations of our Terms of Service, defend against fraudulent claims, or protect the physical security of any individual.
5. **Corporate Restructuring:** In the event of a merger, acquisition, asset sale, or reorganization of Hacktape Technologies Private Limited, user data will transition under the protective covenants of this Privacy Policy.

8. INTERNATIONAL DATA TRANSFERS

Hacktape operates globally. Your information may be transmitted to, stored, and processed in cloud data centers located in India, the United States, and the European Union.

When transferring data across international boundaries, we ensure appropriate legal safeguards:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Adequate technical encryption standards (TLS 1.3 in transit, AES-256 at rest);
- Compliance with the cross-border data transfer directives established under the Indian DPDP Act, 2023.

9. DATA RETENTION AND PURGING

- **Active Accounts:** We retain your account credentials, challenge progress, and billing history for as long as your account remains active.
- **Account Deletion:** You may request account deletion at any time by emailing `privacy@hacktape.io` or initiating deletion via Account Settings. Upon verification, your personal identifiers (name, email, OAuth IDs) are permanently wiped or irreversibly anonymized within thirty (30) days, except where retention is mandated by statutory tax, accounting, or audit laws (typically up to 7 years for financial transaction records).
- **Cryptographic Certificates:** Public certificate verification records remain cryptographically verifiable in perpetuity unless explicitly requested to be revoked by the authenticated recipient.
- **Ephemeral Sandbox Data:** Purged immediately from client memory upon tab closure or VM restart.

10. SECURITY OF YOUR DATA

We implement rigorous physical, administrative, and technical safeguards designed to protect personal data against unauthorized access, destruction, loss, or alteration:

- **Encryption Everywhere:** All traffic is encrypted in transit using Transport Layer Security (TLS 1.3 / HTTPS). Database storage and backups are encrypted at rest using AES-256.
- **Zero-Knowledge Architecture:** Terminal sessions execute inside client-side WASM; no central shell logging.
- **Least-Privilege RBAC:** Production database credentials and secrets are strictly compartmentalized and inaccessible to unauthorized personnel.
- **Regular Security Assessments:** Continuous dependency scanning, static code analysis, and vulnerability mitigation protocols.

11. YOUR PRIVACY RIGHTS (GDPR, CCPA/CPRA, DPDP ACT)

Depending on your geographical location and applicable laws, you hold the following rights:

1. **Right of Access & Portability:** Request a copy of your personal data in a structured, commonly used, machine-readable format.
2. **Right to Rectification:** Request correction of inaccurate, outdated, or incomplete personal data.
3. **Right to Erasure ("Right to be Forgotten"):** Request permanent deletion of your account and associated personal data.
4. **Right to Restrict or Object to Processing:** Object to processing based on legitimate interests or restrict automated processing.
5. **Right to Withdraw Consent:** Where processing is based on consent, withdraw consent at any time without affecting past lawful processing.
6. **Right to Nominate (DPDP Act 2023):** Nominate an individual to exercise your privacy rights in the event of death or incapacity.

To exercise any of these statutory rights, please submit an official request to our Data Protection Officer at `privacy@hacktape.io`. We will acknowledge and respond within thirty (30) calendar days without charge.

12. CHILDREN'S PRIVACY

The Platform is intended exclusively for individuals aged eighteen (18) years or older, or individuals aged at least thirteen (13) years who possess affirmative, verifiable parental or legal guardian consent. We do not knowingly collect personal data from children under the age of 13. If we discover that personal data of a minor under 13 has been collected without verifiable consent, we will delete the data immediately.

13. MODIFICATIONS TO THIS PRIVACY POLICY

We reserve the right to revise or update this Privacy Policy at our sole discretion. In the event of material modifications, we will provide prominent notification by updating the "Last Updated" date at the top of this document, sending an email notice to registered operators, or displaying an announcement banner upon platform login. Your continued use of Hacktape following the effective date of an amended Policy constitutes acceptance of the revised terms.

14. DATA PROTECTION OFFICER & CONTACT INFORMATION

If you have questions, concerns, complaints, or feedback regarding this Privacy Policy or our data protection practices, please contact our Data Protection Officer:

Data Protection Officer (DPO)
Hacktape Technologies Private Limited
Email: `privacy@hacktape.io`
Legal Inquiries: `legal@hacktape.io`
Postal Address: [Registered Office Address, New Delhi, India]
Response SLA: Within 30 calendar days