DEEP
ARMOR

www.deeparmor.com

Privacy Policy

Deep Armor Technologies Private Limited

Effective Date	April 1, 2018
Last Updated	July 14, 2023

Table of Contents

1. Information We Collect 3
2. How We Use Your Information 3
3. Data Retention & Confidentiality 3
4. Special Provision: Penetration Testing & Vulnerability Data 4
5. Security Measures 4
6. Third-Party Sharing 5
7. Your Rights 5
8. Technical Security Controls 5
9. Contact Us 6

At **Deep Armor Technologies Private Limited ("Deep Armor")**, we take security seriously – not just for our customers' networks, but for their data as well. This Privacy Policy explains how we collect, use, and protect your information when you visit our website, engage our consulting services, or communicate with us.

1. Information We Collect

We collect information to provide high-quality security consulting and to improve our service offerings.

- **Information You Provide:** Name, business email, phone number, job title, and company name when you request a quote or consultation.
- **Service Data:** During an engagement (e.g., penetration testing or audits), we may process technical data such as architecture documents, diagrams, test accounts, API documentation, IP addresses, network logs, and system configurations.
- **Vulnerability Information:** Bug and vulnerability reports from other engagements, internal security assessments, bug bounty programs, etc.

2. How We Use Your Information

We use your data strictly for professional purposes:

- To deliver consulting services and security assessment reports.
- To communicate regarding project updates or security vulnerabilities
- To comply with legal obligations and industry standards (e.g., SOC2, ISO 27001).
- To prevent fraudulent activity or unauthorized access to our systems.

3. Data Retention & Confidentiality

As a security firm, we adhere to the principle of **Data Minimization**:

- **Retention:** We only keep customer data for as long as necessary to fulfill the project scope or as required by law.
- **Confidentiality:** All consultant-customer communications are protected by Non-Disclosure Agreements (NDAs). We do not sell your data to third parties.

4. Special Provision: Penetration Testing & Vulnerability Data

Due to the sensitive nature of security assessments, we apply enhanced protections to data handled during penetration tests, red teaming, or vulnerability audits.

- **Data Capture Limitations:** During testing, our consultants follow the "Principle of Least Collection." We aim to prove the existence of a vulnerability without extracting unnecessary Sensitive, Personally Identifiable Information (PII) or proprietary trade secrets.

- **Secure Data Handling:** Any data captured during an engagement (such as database snippets, configuration files, or screenshots) is stored on encrypted, laptops belonging to consultants authorized to work on such engagements.

- **Transmission of Findings:** Final security reports containing sensitive vulnerability data are never sent via unencrypted means. By default, we email the reports to authorized individuals on the customer side. We offer an option to use secure file sharing platforms and/or password protected PDFs.

- **Post-Engagement Sanitization:** Upon the conclusion of the engagement and the expiration of the agreed-upon retention period (typically 30–90 days to allow for client re-testing), we perform a cryptographic erase of all raw data and artifacts collected from your environment. Some customers require us to keep the reports to assist with future engagements. Please inform us in advance if vulnerability reports should be maintained by us.

- **Evidence Logs:** We maintain a strictly controlled log of our testing activities (time stamps, user accounts, test cases and tools used) to provide an audit trail for your internal compliance requirements.

5. Security Measures

We "practice what we preach." Your data is protected by:

- **Encryption:** AES-XTS encryption for data at rest (macOS FileVault) and TLS 1.2+ for data in transit.

- **Access Control:** Strict Multi-Factor Authentication (MFA) and Least Privilege access for our staff.

- **Secure Storage:** Use of AWS cloud environments and Google Workspace for storing & sharing customer data.

6. Third-Party Sharing

We do not share your information except in these limited cases:

- **Service Providers:** Secure tools we use to run our business (e.g. Burp Suite Professional, encrypted CRM, etc.).
- **Legal Necessity:** If required by a court order or to protect our legal rights.

7. Your Rights

Depending on your location (e.g., EU/UK or California), you may have the right to:

- Request a copy of your personal data.
- Request the deletion of your data.
- Opt-out of marketing communications.

8. Technical Security Controls

We implement "Defense in Depth" to ensure that the data you entrust to us, and the vulnerabilities we discover, remain confidential.

Control Category	Specific Implementation	Purpose
Data Encryption	AES-XTS for data at rest; TLS 1.3 for data in transit.	Prevents unauthorized data reading if intercepted or stolen.
Access Management	Google Authenticator MFA & Role-Based Access Control (RBAC).	Ensures only the specific consultants assigned to your project can access your data.
Endpoint Security	Fully encrypted drives and remote wipe capabilities.	Protects data stored on consultant workstations from physical or malware-based theft.
Network Security	Zero-Trust Network Access (ZTNA) and dedicated secure tunnels for testing (Customer's Responsibility)	Isolates testing traffic and prevents lateral movement into our internal business systems.
Data Deletion	NIST 800-88 compliant data sanitization.	Ensures data is irrecoverable after the engagement is finalized.

9. Contact Us

If you have questions about this policy or our data handling practices, please contact:

Deep Armor Technologies Private Limited

Email: privacy@deeparmor.com

Address: Milwaukee – Unit 101, 40 Promenade Road, Sindhi Colony Pulikeshi Nagar, Bengaluru 560005, India