

Privacy Policy

Product: TestRelic **Data Fiduciary:** Techolics Products Private Limited **Registered in:** India
Effective Date: 27 March 2026 **Version:** 1.0.0

1. Identity of the Data Fiduciary

This Privacy Policy describes how **Techolics Products Private Limited**, a company incorporated under the Companies Act, 2013, with its registered office in India ("Company," "we," "us," or "our"), collects, uses, stores, and protects personal data in connection with the TestRelic platform ("Platform") available at **platform.testrelic.ai**.

We act as a **Data Fiduciary** under the **Digital Personal Data Protection (DPDP) Act, 2023** with respect to personal data of individual users, and as a **Data Processor** with respect to personal data contained within Customer Data submitted by organizations.

Data Protection Officer (DPO): privacy@testrelic.ai **Grievance Officer:** legal@testrelic.ai
(see Section 14 for details)

2. Scope and Applicability

This Privacy Policy applies to:

- All individuals who register for, access, or use the Platform at platform.testrelic.ai;
- All visitors to our marketing website at testrelic.ai;
- All digital personal data processed wholly or partly by automated means.

This Policy does not apply to:

- Third-party services or integrations that you connect to the Platform (their own privacy policies govern);
- Customer Data that is purely non-personal (e.g., test run execution logs with no personally identifiable information).

By using the Platform, you agree to the collection and use of information in accordance with this Policy.

3. Data We Collect

3.1 Account and Identity Data

When you register for an account, we collect:

- **Full name**
- **Work email address**
- **Company / organization name**
- **Password** (stored as a one-way cryptographic hash using an industry-standard algorithm; we never store plaintext passwords)
- **Account role** (Admin, Member, Viewer, etc.)

3.2 Organizational Data

When you create or join an organization on the Platform, we collect:

- Organization name and identifier
- List of member email addresses, names, and assigned roles
- Invitation records (email, invite token hash, expiry timestamp)

3.3 Usage and Telemetry Data

To operate and improve the Platform, we automatically collect:

- Test run metadata: run ID, repository name, branch, commit hash, test suite name, pass/fail/skip counts, duration, timestamps
- Pipeline event data: CI/CD event types, SDK version, integration name
- API call logs: endpoint accessed, HTTP status code, response time, timestamp (no request body content retained beyond what is necessary for debugging)
- Authentication events: login timestamps, IP address, device type, browser user-agent (for security monitoring only)
- Error and crash reports: stack traces, affected component (no personal data intentionally included)

3.4 Test Artifact Data

Files and data stored in your organization's designated storage paths (cloud storage buckets and data streams) are your **Customer Data**. We process this data on your behalf as a Data Processor. We do not inspect the contents of test artifacts except as necessary to deliver the service (e.g., indexing metadata for search).

3.5 Communication Data

If you contact our support team, we collect the content of your communications and your contact details for the purpose of responding to your request.

3.6 Payment and Billing Data

Payment transactions are handled directly by our third-party payment processor. We do not store full credit/debit card numbers, CVVs, or bank account details. We retain only:

- Subscription tier and status
- Billing cycle dates
- Payment processor customer reference ID

3.7 Data We Do NOT Collect

We do not intentionally collect:

- Sensitive Personal Data (as defined under Rule 3 of the SPDI Rules 2011) or Sensitive Personal Data under DPDP Act 2023, unless you are in violation of our Terms of Service
- Biometric data
- Data concerning children under 18 years of age

4. Legal Basis for Processing

We process your personal data under the following legal bases as recognized by the **DPDP Act 2023** and the **IT Act 2000**:

Purpose	Legal Basis
Account creation and authentication	Consent (given at sign-up)
Service delivery and platform operation	Contract performance
Billing and payment processing	Contract performance
Security monitoring and abuse prevention	Legitimate interests
Legal compliance and regulatory obligations	Legal obligation
Product analytics (aggregated, anonymized)	Legitimate interests
Marketing communications and product updates	Consent (separately obtained, opt-in)

5. Granular Consent Architecture

In compliance with **Rule 3 of the DPDP Rules, 2025**, we maintain separate, independently withdrawable consent for each distinct processing purpose:

Consent Purpose	Required for Service?	How to Withdraw
(a) Service Delivery – authentication, account management, service operation	Yes (core function)	Close your account
(b) Product Analytics & Improvement – aggregated usage statistics	No	Account Settings → Privacy
(c) Marketing Communications – product updates, newsletters, promotions	No	Email unsubscribe link or Account Settings

Withdrawal of consent for non-essential purposes is as simple as toggling a setting in your account. Withdrawing consent for Service Delivery will result in account closure. Withdrawal does not affect the lawfulness of processing based on consent before withdrawal.

Consent must be **Free, Specific, Informed, Unconditional, and Unambiguous** as required by the DPDP Act 2023. We do not use pre-ticked checkboxes for non-essential consents.

6. AI Features and Model Training

6.1 No Training on Customer Data

Your test run data, pipeline metadata, source code references, artifact content, and any other Customer Data are **never used** to train, fine-tune, benchmark, or improve any artificial intelligence or machine learning model – whether operated by us or by any third party – **without your explicit, separate, written opt-in consent**.

This commitment applies during the term of your subscription and continues after account termination.

6.2 Aggregated Anonymized Improvements

We may use **fully anonymized, aggregated** platform usage statistics (e.g., "what percentage of runs have more than 500 test cases") for internal product improvements. Such statistics contain no personal data and cannot be linked back to any individual or organization.

6.3 Right to Object

You have the right to object to any use of your data for AI/ML purposes at any time by contacting us at privacy@testrellic.ai. We will respond within 30 days.

7. How We Use Your Data

We use the personal data we collect for the following purposes:

- **Authentication and access control:** verifying your identity, issuing and validating session tokens, managing MFA
- **Service delivery:** processing test runs, generating reports, storing results, managing organization memberships and API keys
- **Security and fraud prevention:** detecting unauthorized access, rate-limit enforcement, abuse investigation
- **Customer support:** responding to queries, debugging reported issues
- **Billing and subscription management:** processing payments, managing plan upgrades/downgrades, issuing invoices
- **Platform analytics (aggregated):** understanding feature adoption and performance to improve the Platform; no individual-level profiling
- **Legal compliance:** responding to lawful requests, maintaining audit logs as required by Indian law
- **Communications:** transactional emails (password resets, OTPs, invite notifications) and, with your separate consent, product updates and marketing

We do **not** use your personal data for:

- Automated individual decision-making with legal or significant effects without human review
 - Selling or renting to third parties
 - Targeted advertising
-

8. Data Storage and Infrastructure

8.1 Storage Systems

Your data is stored in the following categories of systems:

Data Type	Storage System	Encryption
Account and organization data	Relational database	AES-256 at rest
Test run metadata	Relational database	AES-256 at rest
Test telemetry and timeline streams	Time-series data store	AES-256 at rest
Test artifact files	Cloud object storage	AES-256 at rest
Transactional emails	Cloud email delivery service	TLS in transit

8.2 Encryption

All data is encrypted:

- **At rest:** AES-256 encryption
- **In transit:** TLS 1.2 or higher for all network communication; HTTP Strict Transport Security (HSTS) enforced

8.3 Hosting Region

Our primary hosting infrastructure is located on **Amazon Web Services (AWS) in the us-east-1 (Northern Virginia) region.**

9. Cross-Border Data Transfers

Your personal data is stored and processed on AWS infrastructure located in the **United States**. This constitutes a cross-border transfer of personal data from India to the United States.

We acknowledge that the DPDP Act 2023 permits the Central Government to restrict cross-border transfers to certain jurisdictions by notification. We will monitor such notifications and take necessary compliance steps within the required timeframes. We use AWS Standard Contractual Clauses and Data Processing Agreements to provide an adequate level of protection for personal data transferred outside India.

If you require data residency within India for compliance or contractual reasons, please contact us at **privacy@testrelic.ai** to discuss Enterprise plan options.

10. Data Retention and Deletion

Data Category	Retention Period
Account data (name, email, company)	Duration of subscription + 90 days after account closure
Test run metadata	Per subscription tier limits (visible in Platform settings)
Test artifact files	Per subscription tier limits
Authentication and security logs	90 days (for security monitoring)
API call logs	30 days
Support communication records	3 years after ticket closure
Billing records	7 years (as required under Indian taxation and accounting laws)

After the retention period expires, data is permanently and securely deleted or irreversibly anonymized. Upon account closure, we provide a **30-day data export window**; after that, deletion proceeds as described above.

You may request early deletion of your personal data at any time (see Section 12 for User Rights). We will confirm deletion within 30 days of a valid request.

11. Right to Erasure and Machine Unlearning

Since we do not use your Customer Data to train AI or machine learning models (Section 6.1), the right to erasure means:

- Deletion of your personal data from our databases (account, organization, audit records)
- Deletion of your test run metadata from our databases
- Deletion of your telemetry and timeline data from our data stores
- Deletion of artifact files from our cloud storage (where stored by us on your behalf)

No model retraining is required because your data has never been incorporated into model weights. We will confirm erasure in writing within 30 days of a valid request.

12. Your Rights under the DPDP Act 2023

Under **Sections 11–14 of the Digital Personal Data Protection Act, 2023**, you have the following rights:

12.1 Right to Access (Section 11)

You may request a summary of personal data we hold about you, the processing purposes, and the list of Data Processors and other Data Fiduciaries with whom we have shared your data.

12.2 Right to Correction and Update (Section 12)

You may request correction of inaccurate or incomplete personal data. Some corrections (e.g., name, company) can be made directly in your account settings.

12.3 Right to Erasure (Section 12)

You may request deletion of your personal data. See Section 10 and Section 11 for details on timelines and scope.

12.4 Right to Grievance Redressal (Section 13)

You may file a grievance with our Grievance Officer (see Section 14). We will acknowledge your grievance within **48 hours** and resolve it within **30 days**. If unsatisfied, you may escalate to the **Data Protection Board of India**.

12.5 Right to Nominate (Section 14)

You may nominate another individual to exercise your data protection rights on your behalf in the event of your death or incapacity. Please contact **privacy@testrellic.ai** to set up a nomination.

12.6 Right to Withdraw Consent

You may withdraw consent for non-essential processing purposes at any time via Account Settings or by contacting us. Withdrawal does not affect the lawfulness of prior processing.

To exercise any of these rights, contact our DPO at **privacy@testrellic.ai** with subject line "Data Rights Request". We may ask you to verify your identity before processing the request.

13. Security Measures

We implement the following technical and organizational security measures:

Technical Measures:

- **Authentication:** Session tokens are stored using secure, server-controlled mechanisms; client-side storage of sensitive tokens is not permitted
- **Password hashing:** Passwords are protected using an industry-standard, memory-hard cryptographic hashing algorithm
- **Database security:** Parameterized queries are used for all database operations to prevent injection attacks
- **Rate limiting:** Applied to all authentication endpoints (login, signup, password reset, OTP) and public API endpoints
- **Transport security:** TLS 1.2 or higher enforced for all communications; HTTP Strict Transport Security (HSTS) enabled
- **Dependency security:** Automated vulnerability scanning runs in our CI/CD pipeline; known high or critical vulnerabilities are blocked from deployment
- **Access control:** Role-based access control (RBAC) within organizations; principle of least privilege for all infrastructure access

Organizational Measures:

- Access to production data limited to authorized personnel on a need-to-know basis
- Security review as part of every feature development cycle
- Incident response plan in place; data breach notification within the timelines prescribed by DPDP Rules 2025

Data Breach Notification: In the event of a personal data breach that is likely to result in harm to you, we will notify the Data Protection Board of India within the prescribed timeframe and notify affected users as required by law.

14. Grievance Officer

In accordance with **Rule 5(9) of the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** and the **DPDP Act 2023**, we have designated a Grievance Officer:

Role: Grievance Officer / Data Protection Officer **Email:** legal@testrelic.ai **Organization:** Techolics Products Private Limited **Country:** India

You may submit a grievance via email with the subject line "Privacy Grievance". We will acknowledge receipt within **48 hours** and resolve the grievance within **30 days** of receipt. If you are not satisfied with our resolution, you may escalate to the **Data Protection Board of**

India (once constituted and operational under the DPDP Act 2023).

15. Third-Party Service Providers

To deliver the Platform, we engage trusted third-party service providers in categories including cloud infrastructure and hosting, email delivery, payment processing, and content delivery. All such providers are located in countries or regions with adequate data protection standards for the purposes of the data shared with them.

We enter into Data Processing Agreements (DPAs) or equivalent contractual arrangements with all third-party providers who process personal data on our behalf. These agreements require providers to handle personal data only on our instructions, implement appropriate security measures, and not use the data for any other purpose.

We will notify you of any material changes to our use of third-party providers that affect the processing of your personal data, with at least 30 days' advance notice where reasonably practicable. You may request a current list of service provider categories by contacting us at **privacy@testrelic.ai**.

16. Cookies and Tracking

16.1 Session Cookies

We use a secure session cookie to maintain your authenticated session. This cookie is essential for Platform operation and cannot be disabled.

16.2 Analytics Cookies

If you consent to Product Analytics (Section 5), we may use first-party analytics to collect aggregated, anonymized usage data. We do not use third-party advertising cookies or cross-site tracking technologies.

16.3 No Third-Party Advertising

We do not display third-party advertisements on the Platform and do not use advertising networks.

17. Children's Privacy

The Platform is not directed to or intended for use by individuals under the age of **18 years**. We do not knowingly collect personal data from children. If we become aware that we have inadvertently collected personal data from a child under 18, we will delete it promptly. If you believe a child has provided us with personal data, please contact us at **privacy@testrelic.ai**.

18. Amendments to This Policy

We may update this Privacy Policy periodically. For **material changes** — including changes to the categories of data collected, processing purposes, or your rights — we will:

- Provide at least **30 days' advance notice** via email to your registered account address;
- Update the "Effective Date" and "Version" at the top of this document;
- Require renewed consent where required by the DPDP Act 2023.

Continued use of the Platform after the effective date of the updated Policy constitutes acceptance of the changes. If you do not agree, you must cease using the Platform and may request account closure before the effective date.

19. Contact Us

For any privacy-related inquiries, requests, or concerns:

Data Protection Officer Techolics Products Private Limited Email: **privacy@testrelic.ai**

Grievance Officer Email: **legal@testrelic.ai** Website: **testrelic.ai**

We will respond to all privacy inquiries within **30 days** of receipt.

This Privacy Policy was last updated on 27 March 2026 and is effective as of the same date.