Technical and Organizational Measures (TOMs)

Purpose: Secure handling of customer data in the context of cross-browser and mobile device testing services.

Date: April 2025

1. Confidentiality

Access Control

- Role-based access control (RBAC) for internal systems.
- Access to production systems is limited to authorized personnel via VPN and SSH keys.
- Multi-factor authentication (MFA) is enforced for all staff accounts.
- Access logs are maintained and reviewed regularly.

Data Encryption

- All data in transit is encrypted using TLS 1.2 or higher.
- Customer test data, including logs and screenshots, are encrypted at rest using AES-256.

Staff Confidentiality

- All employees sign confidentiality and data protection agreements.
- Regular training is provided on data protection and secure development practices.

2. Integrity

Input Control

- API and web UI are protected with authentication and rate limiting to prevent unauthorized manipulation of data.
- Input data validation and sanitation is implemented to avoid injection attacks.

Data Separation

- Customer test sessions are isolated: each test runs on its own single use Virtual Machine.
- Session logs, screenshots, and videos are assigned to unique test identifiers per user/project.

3. Availability and Resilience

Backup and Recovery

- Regular backups are taken of essential infrastructure and customer data.
- Backups are encrypted and stored in geographically redundant locations.
- Disaster recovery plans are tested semi-annually.

High Availability

- TestingBot infrastructure is hosted on highly available cloud environments.
- Automatic failover and load balancing mechanisms are in place for test execution and session management systems.

4. Data Minimization and Retention

Retention Policies

- Test logs, screenshots, and videos are retained for a limited time (default 31 days unless configured otherwise by the customer).
- Users can delete their own test data at any time via the dashboard or API.

Data Disposal

- Secure deletion procedures are followed when removing customer data from storage.
- Disks used for storage are securely wiped or destroyed at the end of their lifecycle.

5. Monitoring and Incident Response

Monitoring

- All systems are monitored for uptime, performance, and unauthorized access attempts.
- Security event logs are centralized and retained for auditing.

Incident Management

- A documented incident response policy is in place.
- Customers are notified of security incidents affecting their data in a timely manner, following GDPR Article 33.

6. Subprocessors

Subprocessor Oversight

- All subprocessors are contractually bound to comply with data protection obligations.
- TestingBot maintains an up-to-date list of subprocessors at https://trust.testingbot.com

7. Audits and Certifications

Compliance

- Regular internal audits are conducted to verify TOMs effectiveness.
- Third-party penetration testing is conducted at least annually.
- TestingBot follows industry best practices aligned with ISO 27001 and GDPR requirements.

8. Customer Control

Configuration Options

- Customers can configure retention settings and access control for their teams.
- API keys and test visibility options (e.g., private tests) give customers granular control.