Privacy Policy for TouchStage Recorder Extension

Last Updated: July 18, 2025

Version: 1.0

1. Introduction

At TouchStage, we value your privacy and are committed to protecting your personal information. This Privacy Policy explains how TouchStage Software Pvt. Ltd. (“TouchStage”, “we”, “our”, or “us”) collects, processes, stores, and protects your information when you use the TouchStage Recorder Chrome Extension (the “Extension”).

This Extension is designed to capture user interactions, API calls, and other relevant session data to help users create guides, troubleshoot workflows, and analyze product usage within their web applications.

We take privacy and security seriously and aim to ensure transparency about what data we collect, why we collect it, and how you can manage it.

---

2. Information We Collect

2.1 Personal Information

When you use the TouchStage Recorder Extension, we collect the following types of personal information:

- **Email Address:** Required when you log in or create an account on the TouchStage platform.

- **Authentication Credentials:** Depending on your organization’s security configuration, we may collect authentication tokens or API keys necessary for verifying session access.

Note: Passwords entered within web pages are never recorded or collected. Password input fields are automatically excluded from all recordings.

2.2 Session Recording Data

When you actively initiate a recording session using the Extension, we capture detailed interaction and network data, including:

- **User Interactions:**
    - Clicks, mouse movements, keyboard inputs (excluding passwords), scroll events, and page navigation events.
    - Element selectors and structural data necessary to recreate the session accurately.
- **Visual Content:**
    - Screenshots of web pages or elements to visually map your workflow.
    - DOM (Document Object Model) structure and hierarchy of the recorded pages.
- **Network Data:**
    - Captured API requests and responses, including:
        - Request URLs, headers, payloads, and response bodies.
        - Status codes, error messages, and API timing data.
    - Traffic monitoring, including AJAX calls, WebSocket events (where applicable), and third-party API interactions (subject to user approval).
    - Debugger Mode (Optional): Captures deeper network logs and error traces when manually enabled.
- **Metadata:**
    - URLs of pages being recorded.

    - Timestamps (start/end of session, actions).
    - Session duration and viewport resolution.
    - Recorded event sequences.

2.3 Technical Information

- **Extension Configuration:**
    - Your user preferences such as shortcut keys, language settings, recording defaults, and other extension configuration options.
- **Session Authentication Tokens (Optional):**
    - Temporary tokens used for maintaining session continuity when interacting with the TouchStage platform.
    - These tokens are securely stored within your browser and expire periodically.

---

3. How We Use Your Information

The information collected by the TouchStage Recorder Extension is used strictly for the following purposes:

3.1 Session Recording and Workflow Creation

- To create visual and interactive guides from your product workflows.
- To capture API call sequences for agent capability generation or debugging.
- To generate and manage step-by-step user walkthroughs or process recordings.

3.2 User Support and Debugging

- Facilitate issue diagnosis by providing your authorized support personnel with necessary logs (only after explicit consent).
- Capture error traces and failed API logs during debugger mode for root-cause analysis.

3.3 Product Development and Quality Assurance

- Analyze usage patterns to improve TouchStage features and fix bugs.
- Enable your teams to refine workflows and training guides using real-world interaction data.

3.4 Account Management and Security

- Authenticate you as a legitimate user of the TouchStage platform.
- Securely manage your recording sessions and synced data within your account.

4. Data Storage and Retention

4.1 Local Storage (Browser-Side)

- All recorded session data (visuals, API traffic, interactions, metadata) is stored locally within your browser's extension storage during recording sessions.
- You, as the user, have full control over local data retention.
- Local data will persist until:
    - You manually delete it from the extension.
    - You choose to sync it with your TouchStage account via our dashboard.
    - You uninstall the TouchStage Recorder Extension.

Note: Local recordings are not automatically transmitted or synced to TouchStage servers without explicit action.

4.2 Server Storage (Optional Sync)

- When you choose to sync a recording session to your TouchStage account:
    - The data is securely transmitted and associated with your authenticated user account.
    - Synced data becomes accessible through the TouchStage platform dashboard.
    - You retain full control over your uploaded data and can delete synced sessions at any time from within the dashboard.

4.3 Data Retention Periods

- **Local Data:** Stored indefinitely in your browser unless deleted by you.
- **Server Data:**
    - Retained as per TouchStage's general data retention policy, which adheres to GDPR-compliant best practices.
    - Retained until:
        - You delete the session from your TouchStage dashboard.
        - Your account is deleted (in which case all associated data is permanently deleted).
- **Account Deletion:** Deleting your TouchStage account will result in the automatic deletion of all your recordings, synced data, and related personal information.

---

5. Data Security

5.1 Encryption

- All data transmissions (including syncing of session recordings) are protected via HTTPS encryption.
- On the server side, stored data is encrypted using industry-standard AES 256-bit encryption.
- Session authentication tokens and API credentials are stored securely within your browser's local storage using secure mechanisms.
- Backend access to sensitive information is strictly restricted via role-based access controls (RBAC).

5.2 Access Controls

- Only you have direct access to your recordings and session data.
- Data stored on our servers is isolated per user account.
- TouchStage employees cannot access your synced data unless:
    - You explicitly share access with our support team for troubleshooting purposes.
    - Required by legal mandate.

5.3 Security Practices

- Regular vulnerability assessments and penetration testing.
- Encryption at rest and in transit.
- Secure authentication protocols (e.g., OAuth, token-based session management).
- Continuous monitoring for suspicious activities and breaches.
- Protection against Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other web-based threats.

---

6. Your Rights and Choices

6.1 Full Control Over Your Data

- **Recording Control:** You initiate and end recording sessions manually.
- **Sync Control:** No session data is sent to our servers unless you explicitly sync it.
- **Deletion Rights:**
    - Local recordings can be deleted from the extension interface.
    - Synced recordings can be deleted from your TouchStage dashboard.
    - You can delete your entire TouchStage account at any time, which will remove all stored data.

6.2 Transparency in Data Collection

- A visible indicator in the extension will clearly show when a recording session is active.
- You have the ability to preview recordings before syncing.
- TouchStage commits to not collecting any hidden or undisclosed data.

---

7. Data We Explicitly Do NOT Collect

- Password field inputs (automatically excluded by the extension).
- Health, financial, or payment-related data.
- Personal communications like emails, messages, or private chat content.
- Browsing history beyond active recording sessions.

- Device identifiers or geolocation data beyond page URLs.
- Audio recordings or microphone access (unless separately authorized for specific features).

8. Data Sharing & Disclosure

8.1 No Third-Party Data Sales

- We do **not** sell, rent, or trade your personal information or recorded session data to any third parties for marketing or commercial purposes.

8.2 Trusted Service Providers

- We may engage third-party service providers to:
    - Host our servers and databases (e.g., AWS, Azure).
    - Provide analytics or diagnostic tools.
    - Assist with technical support and service optimization.

These providers:

- Are contractually bound by confidentiality agreements.
- Can only process your data on our instructions.
- Must comply with strict data protection standards (GDPR, CCPA, etc.).

8.3 Legal Requirements

- We may disclose your data if required to:
    - Comply with applicable legal obligations (court orders, government requests).
    - Protect and defend our legal rights.
    - Prevent fraud or security threats.

We will always assess the necessity and legality of such disclosures.

---

9. International Data Transfers

Your data may be processed in regions outside your own (e.g., EU, US) depending on server location and service providers used.

For such transfers:

- We apply appropriate safeguards as mandated by GDPR, such as:
    - Standard Contractual Clauses (SCCs).
    - Binding Corporate Rules (BCRs).
    - Adequacy decisions (where applicable).

All transfers comply with applicable privacy regulations, ensuring your data remains protected even outside your jurisdiction.

---

10. GDPR & CCPA Rights

10.1 GDPR (For EU Users)

You have the following rights:

- **Right to Access** – View what personal data we store about you.
- **Right to Rectification** – Correct inaccurate or incomplete data.
- **Right to Erasure (Right to be Forgotten)** – Delete your data.
- **Right to Restrict Processing** – Limit how we use your data.
- **Right to Data Portability** – Export your data in a structured format.
- **Right to Object** – Object to processing activities, including automated decision-making.

To exercise these rights, contact us via the details in Section 12.

10.2 CCPA (For California Users)

Your rights include:

- **Right to Know** – Understand what personal information is collected and how it's used.
- **Right to Delete** – Request deletion of personal information.
- **Right to Opt-Out** – Prevent us from selling your data (we do not sell any data).
- **Right to Non-Discrimination** – Equal service regardless of your privacy choices.

Requests can be made through your TouchStage dashboard or via email.

---

11. Changes to This Privacy Policy

We may periodically update this Privacy Policy. Updates will be communicated via:

- Posting the revised version within the TouchStage Recorder Extension interface.
- Updating our website privacy page.
- Email notifications (for registered account holders).

Your continued use of the extension after changes are made constitutes acceptance of the updated policy.

---

12. Contact Information

For privacy concerns, data requests, or complaints, contact us at:

- **Email:** privacy@touchstage.ai
- **Website:** www.touchstage.ai/privacy

- **Address:** TouchStage Privacy Team, Aikolumi Software Pvt Ltd, Kochi, Kerala, India

Data Protection Officer (DPO) Contact (EU-specific):

- **Email:** dpo@touchstage.ai
- **Address:** [EU Representative Address, if required]

---

13. Complaints

If you feel your data rights have not been properly respected, you have the right to lodge a complaint with your local data protection authority.