

Privacy Policy for Yandex Tracker Multi-Time (Unofficial)

Last Updated: June 17, 2026

This Privacy Policy describes how the **Yandex Tracker Multi-Time** Chrome Extension (referred to as "the Extension", an unofficial time-tracking tool) collects, uses, and protects user information.

We value your privacy and are committed to maintaining transparency regarding the data processed by the Extension.

1. What Information the Extension Processes

To provide time-tracking and productivity insights directly integrated with Yandex Tracker, the Extension processes the following types of data:

- **Authentication Data (OAuth 2.0):** The Extension integrates with Yandex Tracker using secure OAuth 2.0 protocol via `chrome.identity.launchWebAuthFlow` interacting with official Yandex OAuth endpoints (`https://oauth.yandex.ru` and `https://oauth.yandex.com`). The Extension securely obtains and stores authorization tokens. **We do not handle, store, or have access to your raw Yandex account credentials (username or password).**
 - **Yandex Tracker Task and Worklog Data:**
 - Task IDs extracted from active tab URLs of Yandex Tracker pages to automatically associate and manage timers.
 - Historical worklog (time-tracking) entries fetched from the Yandex Tracker API (`https://api.tracker.yandex.net`) to display local productivity insights in your analytics dashboard.
 - **Local Session and Timer State:** Timer state, multi-timer queues, and application state used to keep your tracking history intact on your device.
-

2. How the Collected Data is Used

All processed data is used solely to provide and support the core functionality of the Extension, including:

- Creating and managing multiple active timers.
- Automatically detecting task context when you switch tabs on Yandex Tracker pages.
- Displaying local productivity analytics.
- Submitting logged time directly to your Yandex Tracker account.

We **do not collect**, **do not store** on our own servers, and **do not analyze** your personal information, search queries, or browsing history on unrelated websites.

3. Data Storage, Transmission, and Third-Party Disclosure

- **Local Storage:** Your settings, OAuth tokens, active timer states, and local time-tracking history are persisted strictly on your device using Chrome's local storage APIs.
 - **Direct Transmission:** Data is only transmitted over secure HTTPS connections directly to the official Yandex APIs:
 - `https://tracker.yandex.ru/*` and `https://tracker.yandex.com/*` (for UI integration and page interaction).
 - `https://oauth.yandex.ru/*` and `https://oauth.yandex.com/*` (for secure user authentication).
 - `https://api.tracker.yandex.net/*` (for fetching historical worklogs and submitting logged time).
 - **No Third-Party Transmission:** No data is ever transmitted to the developer's server or any third-party analytics and tracking services.
 - **No Selling or Sharing:** We do not sell, trade, or share your data with any external entities.
-

4. Compliance with Chrome Web Store Limited Use Requirements

The Extension's use and transfer of information received from Google APIs (such as local storage and tab permissions) to any other app will adhere to the [Chrome Web Store User Data Policy](#), including the Limited Use requirements:

1. **Allowed Use:** The data is used strictly to provide the core time-tracking, context-detection, and local analytics features as described in the Extension's store listing and user interface.
 2. **Prohibited Transfer:** No user data is transferred to any external party, except for direct transmission to the official Yandex Tracker API to fulfill user-initiated actions.
 3. **Prohibited Advertising:** Under no circumstances will user data be used or transferred for advertising, profiling, or behavioral retargeting.
 4. **Prohibited Human Interaction:** There is no human access or review of your locally stored time-tracking data, authentication tokens, or tab details by the developer or any other entity.
-

5. Technical Safety and Data Security

- **HTTPS Encryption:** All external network API requests are performed over encrypted HTTPS (SSL/TLS) connections to prevent interception.
 - **Heartbeat Monitoring:** To protect against data loss in the event of unexpected browser shutdowns, a local heartbeat monitor runs in the background (every 6 seconds) to save the current timer state securely to your local storage. It does not communicate with external servers.
 - **Permissions Minimization:** The Extension requests only the minimal set of permissions (such as restricted Host Permissions and the Context Menus API) necessary to inject timer UI, update state contextually, and provide context-aware menu options.
-

6. Data Deletion

You can completely remove all data processed by the Extension at any time by:

1. Uninstalling the Extension from Google Chrome.
2. Clearing the browser's extension data in Chrome's settings.

This will instantly delete all local configurations, active timers, cached history, and OAuth authorization tokens.

7. Changes to This Privacy Policy

We may occasionally update this Privacy Policy to reflect changes in our Extension or legal requirements. When updates occur, we will adjust the "Last Updated" date at the top of this page.

8. Contact Information

If you have any questions or feedback regarding this Privacy Policy or your data, please contact us at:

- **Email:** ep@idaproject.com