

# Cookie Policy

Last updated: 19 May 2026

This Cookie Policy explains exactly which cookies and browser storage technologies Cashback Radar (“we”, “us”, “our”) uses on the Platform, why we use them, and how you can manage your choices. This Policy supplements our Privacy Policy and should be read together with it.

## 1. What we use and why

The Platform uses three browser storage items to maintain session continuity between visits: an HTTP cookie, a primary localStorage entry, and a secondary localStorage entry that provides an additional fallback layer. All three store the same pseudonymous visitor identifier and serve as backups for one another. No advertising, marketing, or third-party analytics cookies are set.

## 2. Cookies and storage in use

The table below lists every cookie and browser storage item set by the Platform.

Name	Category	Provider	Duration	Purpose
_cbr_sid (localStorage)	Essential	First-party	Until manually cleared	Secondary session-continuity key. Stores the same pseudonymous visitor identifier as user_token as an additional fallback layer. Used only when both the user_token cookie and the user_token localStorage entry are absent. Cleared when you delete your account via the Platform.
user_token (HTTP Cookie)	Essential	First-party	180 days; renewed on every API request	Pseudonymous visitor identifier. Enables session persistence and the "continue where you left off" feature. HttpOnly, SameSite=Lax, Secure (production).
user_token (localStorage)	Essential	First-party	Until manually cleared	Fallback identifier used when the HTTP cookie is blocked by the browser. The stored value is sent as the X-User-Token request header on every API call.

**No third-party cookies.** The Platform does not load any external advertising, social-media, or analytics tracking pixels.

## 3. Device fingerprint (non-cookie)

In addition to the storage items above, the Platform uses a locally hosted copy of the open-source FingerprintJS v4 library to compute a probabilistic device identifier called a “visitor ID”. The library is served from the Platform’s own domain (no request is made to any external CDN). This identifier is:

- held in JavaScript memory only — never written to a cookie or browser storage;

- sent as the X-FP-Hash request header on every API call;
- used solely as a last-resort fallback to recognise a returning device when all three storage items (cookie, user\_token localStorage, and \_cbr\_sid localStorage) are absent (e.g., private-browsing mode or strict tracker-blocking);
- computed entirely client-side; no data is transmitted to FingerprintJS servers.

FingerprintJS v4 open-source derives its signal from browser and hardware properties (e.g., screen resolution, timezone, installed fonts). It does not set any cookies itself.

#### 4. Server-side session data (not cookies)

All substantive session state — your questionnaire answers, spend-mix estimates, calculation results, consent decisions, and email address (if provided) — is stored server-side in a database, associated with your pseudonymous user\_token. This data does not reside in cookies or browser storage and is therefore not affected by browser cookie controls.

**Transactional email.** If you provide your email address on the Platform (for example, to receive your results or to sign in via magic link), Cashback Radar delivers transactional emails through **Zeptomail**, a service operated by Zoho Corporation Pvt. Ltd. Your email address is transmitted to Zeptomail solely for the purpose of delivering that specific email and is not used by Zoho for any other purpose. Zoho's privacy policy is available at [zoho.com/privacy](https://zoho.com/privacy).

#### 5. Categories explained

**Essential cookies** are strictly necessary for the Platform to function. They do not require consent and cannot be disabled while using the Platform. All items listed in Section 2 fall into this category.

**Analytics (server-side).** When you accept analytics cookies, Cashback Radar logs your interaction milestones (e.g., questions answered, session start/end, results viewed) to its own server-side database for product improvement. This is **not** implemented as a browser cookie; it is a server-side flag tied to your user\_token. No third-party analytics service receives your data.

#### 6. Cookie consent

On your first visit a consent banner is displayed. You may:

- Accept all — enables server-side analytics event logging.
- Manage preferences — toggle the Analytics category individually, then save.

Essential cookies are set unconditionally and cannot be toggled off. Your consent decision is stored server-side (not in a cookie) and is remembered across visits. If you dismiss the banner without making an explicit choice, your preference is recorded as “not decided” and analytics event logging remains disabled; the banner will not re-appear on subsequent visits.

**Withdrawal.** You may withdraw analytics consent at any time by contacting us at [legal@cashbackradar.io](mailto:legal@cashbackradar.io), requesting deletion of your session data. You can also delete your account directly from the Platform's profile menu, which permanently removes all server-side session data and all browser storage items (including \_cbr\_sid) associated with your identity.

Note: deleting individual cookies or localStorage entries via browser settings will terminate your primary session, but a secondary localStorage key (`_cbr_sid`) — also described in Section 2 — may allow session continuity to be re-established on your next visit. To fully reset your identity on the Platform, use the in-app “Delete my account” function, which clears all storage items and server-side data.

Withdrawal does not affect the lawfulness of any processing carried out before withdrawal.

## 7. Browser controls

You can manage cookies through your browser settings at any time. Most browsers allow you to:

- view and delete individual cookies;
- block all cookies or cookies from specific sites;
- clear localStorage entries via Developer Tools.

Note that deleting the `user_token` cookie and localStorage entries will terminate your current session; any in-progress questionnaire answers not yet saved to the server will be lost. See Section 6 regarding the `_cbr_sid` key and full identity reset.

## 8. Security

The `user_token` cookie is set with the following security attributes:

- `HttpOnly` — inaccessible to JavaScript; reduces XSS exposure.
- `SameSite=Lax` — prevents the cookie being sent in cross-site requests initiated by third parties.
- `Secure` — transmitted over HTTPS only (production environment).
- `Path=/` — scoped to the entire Platform.

The `user_token` value is a randomly generated UUID4 and contains no personal data. Email addresses and calculation results are never stored in cookies or localStorage.

## 9. Changes to this Policy

We may update this Cookie Policy to reflect changes in technology, legal requirements, or Platform features. The “Last updated” date at the top of this document will be revised accordingly. Material changes will be communicated on the Platform.

## 10. Contact and data requests

For questions about this Cookie Policy, to request deletion of your session data, or to exercise any other data rights:

### Data Protection Officer

[legal@cashbackradar.io](mailto:legal@cashbackradar.io)

Cashback Radar · IC 19209002 / DIC CZ8507081583

Pod Barvirkou 3348/11, 150 00, Prague 5 – Smíchov, Czech Republic