NestLab

NestLab / Cookie Policy

Cookie Policy

Last updated: 2026-08-09 · Effective: 2026-08-09

Download PDF

1. What cookies we use

This site uses one cookie, set by Cloudflare:

1.1 `_cfuvid` — functional, no consent required

- **Purpose:** Distinguishes between humans and automated traffic. Helps Cloudflare detect bots and abusive requests.
- **Provider:** Cloudflare, Inc.
- **Type:** Functional / security
- **Duration:** Session (cleared when you close the browser)
- **Consent required:** No. Per ePrivacy Directive Art. 5(3), cookies strictly necessary for the operation of the service do not require consent.

1.2 `nestlanding_consent` — essential localStorage, no consent required

- **Purpose:** Records your privacy preferences (which non-essential scripts you accept). Necessary for the consent layer to remember a choice across visits, per Art. 7(1) of the GDPR.
- **Provider:** NestLab (first-party)
- **Type:** localStorage, not a cookie. Listed here because it is the canonical "essential storage" entry alongside the Cloudflare cookie above.

- **Duration:** 12 months from the last change.
- **Consent required:** No. The information is necessary to operate the consent mechanism itself.

1.3 `nestlanding_consent__consent_version` — essential localStorage, no consent required

- **Purpose:** Records the version of this policy that you consented to. A version mismatch forces a re-prompt so the choice always reflects the current policy text.
- **Provider:** NestLab (first-party)
- **Type:** localStorage.
- **Duration:** 12 months from the last change.
- **Consent required:** No.

1.4 Contact form — no cookies, transient form state in sessionStorage

The contact form on `/contact.html` sets NO cookies and stores NO persistent client-side state outside the two essential localStorage entries above. It does, however, use `sessionStorage` as a transient scratch space so a long message is not lost when the server returns an error (see §1.5). Rate limiting is enforced at the Cloudflare edge by a transient IP-based counter (discarded within 24 hours); no fingerprinting, no device ID, no cross-site identifier.

1.5 `contact-draft:*` — transient form draft, sessionStorage, no consent required

- **Purpose:** Preserves the visitor's form input across the no-JS fallback path. When the Worker cannot deliver the message (rate limit, upstream email failure, etc.) it 303-redirects the visitor back to `/contact.html?error=<code>&topic=<t>`. The inline script on `/contact.html` reads the previous values from `sessionStorage` and re-fills the form so the visitor does not have to retype a long message. The script also writes the values back to `sessionStorage` on every keystroke.
- **Provider:** NestLab (first-party)
- **Type:** `sessionStorage`, not a cookie. Listed here for transparency alongside the localStorage entries above.

- **Storage shape:** One key per (topic, field) pair — `contact-draft:<sales|support>:<name|email|company|message>` → field value (string).
- **Duration:** Cleared automatically when the tab or browser is closed. Cleared earlier on a successful submission and as a safety measure on `/thank-you.html` load.
- **Consent required:** No. The information never leaves the visitor's browser — it is read and written only by scripts on `nestlab.tech/contact.html` and is never transmitted to a server, third party, or analytics endpoint. It does not identify the visitor, is not shared, and is not used for tracking, analytics, or advertising. The data is functionally necessary to recover from a server-side failure without forcing the visitor to retype their message.

2. How consent is collected (EU/UK visitors)

We detect which country you are visiting from by reading the country code that our network edge already attaches to every request. We use it for one thing only: deciding whether to show the consent banner on your first visit. Visitors from the EU, UK, Switzerland, or Brazil see the banner on their first visit; visitors from anywhere else do not. The country signal is not stored, not logged as part of the consent decision, and disappears as soon as the banner has decided what to show.

The banner gives you a real choice:

- **Accept** and **Reject** are two buttons with the same size, contrast, and position. Neither is hidden behind a "Settings" link. Either button completes the choice in one click.
- You can close the dialog with the `Esc` key or by clicking outside the dialog. That counts as Decline — not as silent consent.
- You can change your mind later from the **Manage preferences** link in the footer of every page. Withdrawing a previous choice is as easy as making it.
- The dialog traps keyboard focus while it is open and moves focus through its controls in the order you read them, so the choice is reachable without a mouse.

The settings dialog exposes three categories. Each one controls a distinct type of script that might run on this site:

- **Essential** — always on, you cannot turn it off. It covers the consent mechanism itself and the anti-abuse check on the contact form. We treat these as strictly necessary under ePrivacy, so they do not require your consent.
- **Analytics** — opt-in for EU/UK/CH/BR visitors, off by default; opt-out for visitors elsewhere (their default is on). Flipping this on activates PostHog (cookieless, EU region). See §4 for full details.
- **Preferences** — opt-in for EU/UK visitors, off by default. No script is gated under this category today; the toggle is present so the dialog schema is stable when the first such script is added.

Until you choose, nothing runs except the essential scripts above. No analytics, no marketing, no pixels, no third-party trackers. After you choose, we record the decision and the policy version you consented to in your browser. If we ever change this policy in a way that affects what you agreed to, you will be asked again — you are never silently re-bound by a version of the policy you never saw.

If you have an analytics blocker or similar browser extension, the same rules apply: nothing non-essential runs until you have made a choice in this dialog.

3. What we do not use

Today: no marketing pixels, no third-party trackers, no advertising identifiers, no A/B testing tools, no contact-form cookies, no contact-form localStorage beyond the two essential entries, no fingerprinting, no cross-site identifiers. The analytics script (§4) is cookieless by design, gated behind consent, and stores nothing client-side. The `contact-draft:*` `sessionStorage` entries (§1.5) are first-party, per-tab, and never leave the browser.

4. Analytics we use

Since the cookie banner shipped, the only analytics on this site is:

- **Provider:** PostHog, Inc. — PostHog Cloud, EU region (`eu.i.posthog.com`).
- **Purpose:** cookieless product analytics — page views, referrer, country, viewport size, custom events fired from this site. Used to understand which

pages convert and which pages lose visitors. No session recording, no feature-flag delivery, no surveys, no A/B tests.

- **Data:** no PII, no cookies, no localStorage writes, no fingerprinting. PostHog's `disable_persistence: true` + `person_profiles: "never"` config means the script never identifies a visitor and never persists anything client-side. Each page load produces a fresh anonymous identifier that is never stored, so events cannot be linked across page loads or across visits.
- **EU residency:** data is stored and processed in PostHog's EU region (Frankfurt). PostHog acts as our processor under a DPA covering EU SCCs.
- **Retention:** 90 days (PostHog default for cookieless events).
- **Cookies set:** none. Confirmed by the `disable_persistence: true` configuration, which turns off cookie, localStorage and sessionStorage writes.
- **Consent:** the script tag stays `type="text/plain"` on every page until you accept the Analytics category in the consent banner. The script is only activated (cloned into a real `<script>` and executed) after you opt in. Reject All keeps it inert. The decision is persisted in the essential `nestlanding_consent` localStorage entry (§1.2) and you can change your mind any time from *Manage preferences* in the footer.
- **DPA:** posthog.com/dpa. Standard Contractual Clauses apply for the underlying transfer.

5. Your browser controls

You can clear cookies and block cookies through your browser settings. Blocking `_cfuvid` may cause Cloudflare to challenge some requests as suspicious; this is intentional and applies to all sites on Cloudflare.

You can withdraw analytics consent at any time via *Manage preferences* in the footer. Withdrawal is one click — same prominence as the original accept.

6. Cross-site behavior

Our product pages (euaigap.co, tunecv.co, checkcv.co, propvectorai.com) are separate domains with their own cookie policies. This policy covers only `nestlab.tech`.

Changelog

- 2026-07-31 — Initial publication. Phase A: Cloudflare functional only.
- 2026-08-01 — Affirmed contact form sets no cookies; rate limiting is transient IP-based at the edge.
- 2026-08-04 — Documented `contact-draft:*` `sessionStorage` entries (§1.5) used to preserve form input across the no-JS fallback path. Updated §1.4 and §3 to reflect the transient sessionStorage use.
- 2026-08-07 — Documented the consent banner mechanism in §2: symmetrical Reject All paired at the same visual prominence as Accept (single click each, no Settings gate), granular per-category toggles (Essential locked on, Analytics opt-in for EEA/UK/CH/BR, Preferences opt-in for EEA/UK), region-aware defaults, persistent withdrawal via the footer *Manage preferences* link (present on every page), policy-version re-prompt on bump, and the keyboard-Esc / click-outside = Decline (Art. 7(3) withdrawal) treatment. Cross-referenced the byte-equivalent SSOT module `/assets/js/consent-contract.js`. An automated pre-release check asserts the gating plumbing on every HTML page (region meta, analytics placeholder, consent script load, footer preferences link), so the layering holds without per-page review.
- 2026-08-08 — Rewrote §2 in behavior-level language for a non-technical EU visitor. Removed engineering jargon (CF-IPCountry, x-nestlab-region meta tag, regex rewrite, clone-and-append, Object.freeze). Kept the regulatory citations (ePrivacy Art. 5(3), GDPR Art. 7(3)) and the operational facts (region-detected banner, Accept/Reject symmetric, focus trap, footer Manage preferences link, policy-version re-prompt, no non-essential script before consent). The technical mechanism is unchanged — only the policy's wording for visitors changed.
- 2026-08-09 — Replaced the forward-commitment §4 ("when we add analytics") with a concrete §4 describing the PostHog EU cookieless integration actually shipped. Renumbered §4→§5 (browser controls) and §5→§6 (cross-site behavior) to absorb the new section. Updated §2 (Analytics category description) and §3 (What we do not use) to remove the now-stale "no analytics script ships" claims. Added §5 paragraph on withdrawal via Manage preferences.