Detailed Cookie Audit Checklist

Under EU/UK rules, valid consent must be a real affirmative choice; pre-ticked boxes and “scroll/swipe to consent” are not valid consent patterns, and CNIL has repeatedly enforced the principle that refusing cookies should be as easy as accepting them. In the UK, advertising-related storage/access technologies require consent and are not covered by the “strictly necessary” exception. In California, “sharing” for cross-context behavioral advertising is its own concept, so cookie/tracker audits should also check opt-out mechanics for ad-tech flows. (ICO)

Below is the **master checklist content**.

Section A - Scope, inventory, and setup

CA-01 - Define audit scope

Check which domains, subdomains, locales, logged-in states, and environments are in scope.
Evidence: scope note, test matrix.
Risk: Medium.

CA-02 - Identify applicable regulatory regimes

Record whether the site targets or serves EU/EEA, UK, California, and other regions.

Evidence: geo-targeting logic, market list, legal applicability note.

Risk: High.

CA-03 - Identify all consent technologies in use

Document CMP, custom banner, tag manager consent mode, server-side tagging, SDKs, and anti-fraud tools.

Evidence: source code, tag inventory, vendor list.

Risk: High.

CA-04 - Build cookie and tracker inventory

List cookies, local storage keys, session storage items, pixels, scripts/tags, web beacons, fingerprinting signals, and link-decoration/tracking parameters.

Evidence: DevTools Application tab, network log, HAR, vendor docs.

Risk: High.

Why it matters: official UK guidance explicitly treats several non-cookie mechanisms as storage/access technologies, so a cookie audit should not stop at cookies alone. (ICO)

CA-05 - Classify each technology by purpose

Necessary, preferences, analytics, advertising/marketing, personalization, security, fraud prevention, measurement, session replay, etc.

Evidence: inventory sheet, policy mapping, vendor config.

Risk: High.

CA-06 - Identify first-party vs third-party placement/access

Document whether identifiers are set by your domain, embedded vendors, or through server-side proxies.

Evidence: cookie domain attributes, request endpoints, server-side tagging config.

Risk: High.

Section B - Banner and consent interface

CA-07 - Banner appears on first visit where required

Check whether the banner is shown on first visit in relevant regions and contexts.

Evidence: fresh-browser screenshots, geo-based test results.

Risk: High.

CA-08 - Consent request is explicit and affirmative

Check that acceptance requires a clear positive action.

Evidence: UI screenshots, click path.

Risk: High.

Why it matters: valid consent under EDPB guidance must be an unambiguous affirmative act. (EDPB)

CA-09 - No pre-ticked boxes or pre-enabled toggles for non-essential tracking

Evidence: banner screenshots, preferences modal screenshot.

Risk: High.

Why it matters: Planet49 and EDPB guidance make clear that pre-ticked consent is not valid. (infocuria.curia.europa.eu)

CA-10 - No “scroll/swipe/continue browsing = consent” logic

Evidence: UI test recording, consent logic notes.

Risk: High.

Why it matters: EDPB guidance specifically flags scrolling/swiping as invalid consent examples. (EDPB)

CA-11 - Reject option is as easy as accept option

Check button prominence, clicks required, placement, contrast, and path complexity.

Evidence: screenshots, click-count comparison.

Risk: High.

Why it matters: CNIL enforcement repeatedly focuses on refusal being as easy as acceptance. (cnil.fr)

CA-12 - No deceptive design / dark patterns

Check whether colors, wording, button hierarchy, repeated prompts, or friction pressure users into “accept.”

Evidence: screenshots, UX review notes.

Risk: High.

Why it matters: both EDPB and CNIL have addressed manipulative consent patterns. (EDPB)

CA-13 - Granular choices are available where needed

Check whether users can choose categories rather than only “accept all.”

Evidence: settings modal screenshots.

Risk: Medium.

CA-14 - Banner text identifies purposes clearly

Check whether purposes are understandable, specific, and not hidden behind vague language.

Evidence: banner text, policy wording.

Risk: High.

CA-15 - Vendor-level information is available where relevant

Check whether users can see which third parties are involved and for what purpose.

Evidence: settings screen, vendor list, policy links.

Risk: Medium.

Section C - Pre-consent technical behavior

CA-16 - No non-essential cookies set before consent

Evidence: cookie table before interaction, HAR, DevTools Application tab.

Risk: High.

Why it matters: UK and French guidance both center on blocking non-essential tracking before consent. (ICO)

CA-17 - No analytics scripts load before consent

Check GA, GA4, GTM-triggered analytics, Mixpanel, Heap, Amplitude, etc.

Evidence: network requests before consent, tag manager preview.

Risk: High.

CA-18 - No advertising / remarketing scripts load before consent

Check Meta Pixel, Google Ads, TikTok, LinkedIn, X, Snapchat, programmatic ad tech.

Evidence: network log, pixel debugger, HAR.

Risk: High.

Why it matters: advertising-related storage/access requires consent under ICO guidance and is not “strictly necessary.” (ICO)

CA-19 - No third-party identifiers sent before consent

Check IP-linked requests, cookie IDs, click IDs, hashed emails, user IDs, device identifiers.

Evidence: request headers, query strings, payload samples.

Risk: High.

CA-20 - Tag manager respects consent state

Check that GTM / Tealium / Segment / server-side tagging does not fire disallowed tags before consent.

Evidence: consent mode config, tag firing screenshots, request waterfall.

Risk: High.

CA-21 - Consent mode does not mask non-compliant behavior

Check whether “denied” defaults still trigger storage, pings, or equivalent identifiers beyond what is allowed.

Evidence: network logs, vendor docs, implementation notes.

Risk: High.

CA-22 - Local storage / session storage are audited too

Check whether identifiers or tracking state are stored there before consent.

Evidence: browser storage inspection.

Risk: High.

Why it matters: storage/access technologies are broader than cookies. (ICO)

CA-23 - Device fingerprinting or probabilistic identification is assessed

Check whether scripts collect device/browser attributes to identify or track users.

Evidence: script review, network payloads, vendor documentation.

Risk: High.

Why it matters: ICO guidance explicitly includes device fingerprinting, and the ICO has recently taken a strong position against fingerprinting replacing third-party cookies. (ICO)

CA-24 - Link-decoration / navigational tracking is assessed

Check query parameters and redirects that persist identifiers across journeys.

Evidence: network trail, URL parameter inventory.

Risk: Medium.

Why it matters: ICO guidance now explicitly includes link decoration and navigational tracking in this family of technologies. (ICO)

Section D - Post-consent behavior and consent-state changes

CA-25 - Accepting consent enables only the categories selected

Evidence: before/after HAR comparison, tag firing report.

Risk: High.

CA-26 - Rejecting consent keeps non-essential tracking blocked

Evidence: reject-path HAR, cookie table after reject, network log.

Risk: High.

CA-27 - Withdrawing consent actually stops future tracking

Check whether revocation disables future tags and resets consent state.

Evidence: consent change test, network log after withdrawal.

Risk: High.

CA-28 - Previously set identifiers are handled appropriately after withdrawal

Check whether non-essential cookies are removed or disabled where the implementation claims this.

Evidence: cookie comparison, vendor behavior notes.

Risk: Medium.

CA-29 - Consent persists consistently across pages and sessions

Check whether state is remembered accurately without re-triggering disallowed tags.

Evidence: multi-page test, repeat-visit test.

Risk: Medium.

CA-30 - Cross-device / logged-in tracking flows are assessed

Check whether accepting or rejecting on one surface affects tracking on another in a way you disclose.

Evidence: account tests, device tests, vendor mapping.

Risk: Medium.

Section E - Disclosure and documentation

CA-31 - Cookie policy exists and is reachable from the banner

Evidence: banner links, footer links.

Risk: Medium.

CA-32 - Cookie policy matches observed technologies

Check names, purposes, categories, durations, and vendors against real findings.

Evidence: cookie inventory vs policy comparison.

Risk: High.

CA-33 - Privacy policy reflects third-party data sharing and ad-tech behavior

Evidence: policy comparison against network evidence.

Risk: High.

CA-34 - Durations / expiry windows are documented accurately

Evidence: observed cookie attributes, policy entries.

Risk: Medium.

CA-35 - Legal basis / consent wording is internally documented

Evidence: internal compliance memo, RoPA, legal notes.

Risk: Medium.

CA-36 - Change log exists for CMP and tracking changes

Evidence: release notes, CMP version history, tag manager history.

Risk: Medium.

Section F - Third parties, contracts, and regional logic

CA-37 - Third-party vendor list is complete

Evidence: vendor inventory, tag list, procurement record.

Risk: High.

CA-38 - Roles are identified correctly

Check controller / processor / service provider / contractor / third party positions internally.

Evidence: DPA / contract summary, legal review note.

Risk: High.

CA-39 - Cross-context behavioral advertising flows are mapped for California

Check whether pixels, clean rooms, audiences, retargeting, enrichment, or ad measurement create “sharing” or sale/opt-out issues.

Evidence: data flow map, vendor contracts, signal testing.

Risk: High.

Why it matters: California law treats “sharing” for cross-context behavioral advertising as a distinct concept that must be audited. (California DOJ)

CA-40 - Opt-out / choice signals are honored where applicable

Check whether California opt-out paths and browser/global privacy signals are implemented where claimed.

Evidence: preference center tests, request/response behavior, policy review.

Risk: High.

CA-41 - Geo-based behavior is consistent with policy

Check EU/UK vs US vs rest-of-world behavior.

Evidence: VPN/geo tests, screenshots, HAR by region.

Risk: High.

CA-42 - Embedded third-party tools are assessed separately

Check chat widgets, video players, maps, social embeds, A/B testing, CDPs, affiliate tools, session replay.

Evidence: page-by-page inventory, network logs.

Risk: High.

Section G - Evidence and auditability

CA-43 - Evidence package is reproducible

Evidence: timestamped screenshots, HAR files, network logs, cookie tables, browser/version info, geo info.

Risk: High.

CA-44 - Findings are linked to exact page URLs and user flows

Evidence: page inventory, flow notes, screenshots.

Risk: Medium.

CA-45 - Each finding has a severity and remediation note

Evidence: final report, remediation tracker.

Risk: Medium.

CA-46 - Testing covers first visit, reject path, accept path, and settings-change path

Evidence: scenario matrix.

Risk: High.

CA-47 - Testing covers mobile and desktop where implementations differ

Evidence: device/browser matrix.

Risk: Medium.

CA-48 - Testing covers authenticated and anonymous states where relevant

Evidence: user-state matrix.

Risk: Medium.