CONSENTR

PRACTITIONER CHECKLIST

GDPR Compliance Checklist

15 pre-launch steps for UK & EU websites. One-line tests, clear pass/fail criteria.

Published by Consentr • consentr.co.uk • 2026 edition

How to use this checklist

This is a 15-step pre-launch checklist for any commercial website operating in the UK or EU. Each step has a one-line test and a pass/fail criteria. If you can tick all 15, you are in good shape.

Section A — Cookies & tracking (steps 1–6)

1. Cookie audit complete

Run a full scan of every cookie set on first page load and after acceptance. Test: open DevTools → Application → Cookies. Pass: every cookie is documented in your registry.

2. Non-essential cookies blocked before consent

Open the site in an incognito tab. No analytics, ad, or marketing cookies should appear before you click Accept. Pass: only strictly-necessary cookies present.

3. Consent banner visible on every entry page

The banner must show on first visit to *any* page, not just the homepage. Pass: visit /any-deep-link in incognito and the banner appears.

4. Reject is as easy as Accept

Both buttons present at the same level, same prominence. Hiding "Reject" behind "Manage preferences" is non-compliant. Pass: visual parity between the two CTAs.

5. Granular categories available

Users can opt in/out per category (Essential / Analytics / Marketing). Pass: a Preferences panel exists with toggles per category.

6. Consent stored with timestamp + version

You can prove what a specific user consented to and when. Pass: a consent log table exists in your CMP with action, timestamp, and policy version.

Section B — Privacy notices (steps 7–10)

7. Privacy policy is current and findable

Updated within the last 12 months, accessible from every page. Pass: footer link present site-wide.

8. Lawful basis stated for every processing purpose

Each purpose (e.g. marketing, analytics, account) names its lawful basis. Pass: explicit list with consent / contract / legitimate interest mapped per purpose.

9. Third-party processors named

Google, Meta, Stripe, etc. all listed in your privacy policy with link to their notices. Pass: a "Who we share data with" section exists.

10. Data retention periods defined

Users can see how long each category of data is kept. Pass: a retention table exists in your privacy policy.

Section C — User rights (steps 11–13)

11. Subject Access Request (SAR) workflow

A documented process to respond within 30 days. Pass: a privacy@yourdomain.com inbox is monitored and a template response exists.

12. Right to erasure operational

You can fully delete a user's data on request, including from backups within reasonable timeframes. Pass: a deletion checklist covers DB, analytics, marketing tools, and CRM.

13. Marketing opt-out works

Every marketing email has a one-click unsubscribe and the request is processed. Pass: test by subscribing then unsubscribing, confirm no further emails.

Section D — Governance (steps 14–15)

14. DPA registered (where required)

In the UK, register with the ICO and pay the data protection fee. Pass: ICO registration certificate on file.

15. Breach response plan

72-hour notification process documented and tested. Pass: a written runbook exists with named escalation contacts.

> **This checklist is a starting point, not a substitute for legal advice.** Consentr is a tool, not a law firm. For complex processing or high-risk data, engage a qualified DPO or legal counsel.

Common mistakes that fail step 4

- "Accept" button styled as primary, "Reject" as muted link — counts as nudging
- Reject hidden behind a "Settings" or "Manage" click
- Pre-ticked optional categories — explicitly forbidden under GDPR
- No way to withdraw consent after acceptance — must be as easy as giving it
- Banner that re-shows on every page until accepted — coercive