FREE CHECKLIST · 20 POINTS · 2026 EDITION

Ship it. Don't get sued.

The legal & compliance checklist for apps you built fast with AI.

How to use this: go through it before launch, and again before every major release. Tick each box only when it's **live in production**, not just "on the list". Most items take under an hour; together they close the gaps AI app builders usually skip.

5 areas: Legal pages · Consent & data · Honest UX · Accessibility · Ops & user rights



Afeez Badmos
@afeez_sdbytes · SoftwareDevBytes × GMSS

General information, not legal advice. Laws vary by country and state; talk to a lawyer about your specific app.

Legal pages 01-04

- [ ] 01 **Privacy policy**
If you collect any personal data (even just an email), you need one. The Apple App Store and Google Play both require a privacy policy link, and California's CalOPPA requires one for sites and apps that collect personal info from California residents.
DO Publish it at /privacy and link it in the footer, at signup and in your store listing. Say what you collect, why, who you share it with, how long you keep it, and how to contact you.

- [ ] 02 **Terms of service**
Sets the rules of use, limits your liability, and defines governing law and how disputes are handled.
DO Show "I agree to the Terms" with a checkbox or button at signup (clickwrap), and keep old versions with dates.

- [ ] 03 **Refund & cancellation policy**
Payment processors and app stores expect clear refund terms. Many US states (California, for example) have automatic-renewal laws that require clear subscription terms and easy cancellation.
DO State the refund window and exactly how to cancel. Make cancelling as easy as signing up.

- [ ] 04 **Cookie policy**
If you have EU/UK visitors, you must explain which cookies and trackers you use and why.
DO List each cookie or tracker (analytics, ads, chat widgets), its purpose and lifetime, and how to opt out.

Consent & data 05-08

- [ ] 05 **Cookie consent banner**
In the EU/UK, non-essential cookies (analytics, advertising) need opt-in consent before they load, and "Reject" should be as easy as "Accept".
DO Block analytics and ad scripts until the user consents, and keep a record of each consent.

- [ ] 06 **Form consent**
Consent must be a clear, active choice. Pre-ticked boxes don't count under GDPR. Marketing texts in the US generally need prior express written consent (TCPA).
DO Use unticked checkboxes, keep marketing consent separate from accepting the Terms, and save a timestamp of each consent.

- [ ] 07 **Collect only what you need**
Data minimisation is a core GDPR principle, and every extra field you hold is extra liability if you're breached.
DO Delete form fields you don't use (date of birth, address, ID numbers). Set a retention period and purge old data.

- [ ] 08 **Audit third-party SDKs**
You're responsible for what your SDKs collect. Apple's privacy labels and Google Play's Data safety form must include data collected by third parties.
DO List every SDK and API (Stripe, analytics, AI APIs, plugins) and what data each one receives. Sign data processing agreements and disclose them in your privacy policy.

Honest UX 09-12

- [ ] 09 **No dark patterns**
Regulators treat manipulative design as deceptive. Under California's privacy law, "consent" obtained through dark patterns isn't valid consent.
DO Remove confirm-shaming, hidden "decline" links, fake countdown timers and roach-motel signups.

- [ ] 10 **No hidden fees**
The FTC's fee rule (in effect since May 12, 2025) requires all-in pricing for live-event tickets and short-term lodging. Elsewhere, surprise fees can still be deceptive under the FTC Act and state laws such as California's.
DO Show the total price, including mandatory fees, up front, not at the last checkout step.

- [ ] 11 **No fake reviews**
The FTC's rule banning fake reviews and testimonials (in effect since October 2024) lets it seek civil penalties. It covers AI-generated reviews too.
DO Delete placeholder or AI-written testimonials. Only show real reviews, and disclose any incentives.

- [ ] 12 **No unsupported claims**
Marketing claims need proof. Claims like "#1", "bank-level security", "HIPAA compliant" or "AI that guarantees results" can draw FTC scrutiny if you can't back them up.
DO Cut or reword any claim you can't support with data, an audit or a certification.

Accessibility 13-14 · 19

- [ ] 13 **Accessible text & colour contrast**
WCAG 2.1 AA, the usual benchmark in ADA website lawsuits, requires a contrast ratio of at least 4.5:1 for normal text (3:1 for large text). The European Accessibility Act has applied to many consumer digital services since June 28, 2025.
DO Run Lighthouse or axe, fix contrast failures, and give every input a label.

- [ ] 14 **Keyboard navigation**
Everything must work without a mouse (WCAG 2.1.1). AI-generated UIs often break this with clickable elements.
DO Tab through every screen: focus should always be visible and modals should trap focus.

Ops & user rights 15-20

- [ ] 15 **Show your business details**
Users, payment providers and app stores expect to see who runs the app. EU law requires trader identity details, and US marketing emails need a physical postal address.
DO Add your legal entity name, contact email and address on a Contact or About page and in the footer.

- [ ] 16 **Parental consent for kids' data**
COPPA requires verifiable parental consent if your app targets children under 13 or you knowingly collect their data. The FTC's amended COPPA Rule has a compliance deadline of April 22, 2026.
DO Add an age gate. If kids are part of your audience, get a COPPA review before launch.

Ops & user rights, continued 17–20

- [ ] 17 **Unsubscribe links in every email**
CAN-SPAM requires a clear opt-out in every commercial email, honoured within 10 business days, plus your physical address.
DO Add a one-click unsubscribe link and suppress unsubscribed contacts automatically.

- [ ] 18 **License your fonts, images & code**
AI builders pull in fonts, stock photos, icons and open-source packages. Using them without the right licence is copyright infringement.
DO Keep a licence list: fonts (OFL or commercial), images (paid or free licence), and code (check GPL/AGPL obligations).

- [ ] 19 **Alt text on images**
Screen readers need text alternatives for meaningful images (WCAG 1.1.1). This is one of the most common failures cited in accessibility complaints.
DO Write descriptive alt text for meaningful images and use alt="" for purely decorative ones.

- [ ] 20 **Data deletion option**
Apple requires in-app account deletion for apps that let users create accounts, and Google Play requires a deletion path both in the app and on the web. GDPR and California law also give users a right to delete their data.
DO Add Settings → "Delete my account & data", confirm the request, and actually purge the data, including backups, on a set schedule.

18–20 ✓
Launch-ready. Re-check before each major release.

12–17 ✓
Fix the gaps in legal pages and consent first.

< 12 ✓
Don't run paid traffic yet. Close the gaps before you scale.

WANT IT DONE FOR YOU?

Get a launch-readiness review of your vibe-coded app.

Global McLien Software Solutions reviews AI-built apps for security, accessibility and these compliance gaps, then fixes them. We do the engineering, and you take the legal questions to your lawyer.

globalmcliensoftwaresolutions.com →

Sources: FTC fake reviews rule: ftc.gov · Amended COPPA Rule: federalregister.gov · Apple account deletion: developer.apple.com · FTC fee rule: foley.com · CAN-SPAM guide: ftc.gov · WCAG 2.1: w3.org

This checklist is general information for educational purposes, not legal advice, and doesn't create an attorney–client relationship. Requirements depend on where you and your users are, what data you collect, and your industry. Have a qualified lawyer review your policies before launch. © 2026 Afeez Badmos / SoftwareDevBytes · Global McLien Software Solutions.