CYBER RESILIENCE ACT · CHECKLISTE

20 Prüffragen für Hersteller & App-Anbieter

Alle Pflichten aus dem Cyber Resilience Act entlang des Produktlebenszyklus – von Design über Entwicklung und Release bis Betrieb und Meldewesen. Zu jedem Punkt steht, bis wann er stehen muss und wer ihn typischerweise löst.

STAND
08/2026

IMMER AKTUELL UNTER
flutterapps.agency/cyber-resilience-act/checkliste

SO LEST IHR DIE MARKIERUNGEN

`Frist 09/2026` Meldepflichten – gelten ab dem 11. September 2026 auch für euer heutiges Portfolio.

`Frist 12/2027` Volle Anforderungen – ab dem 11. Dezember 2027.

`Zuständig: …` Wer den Punkt typischerweise löst: ihr intern, eure Kanzlei oder euer Entwicklungspartner.

`[teils Hardware]` Nur für Produkte mit Gerät – reine Apps überspringen den Punkt.

01 Design & Konzeption

4 Punkte

- [ ] 1 **Gibt es eine dokumentierte Cybersicherheits-Risikobewertung, die euer Gesamtprodukt betrachtet – App, Backend und ggf. Gerät?**
  Sie ist das Fundament des CRA: Jedes „gilt für uns nicht“ ist nur mit Begründung in dieser Bewertung zulässig.
  `Frist 12/2027` `Zuständig: Intern, Entwicklungspartner`

- [ ] 2 **Ist geklärt, in welche CRA-Produktklasse euer Produkt fällt – Standard, „wichtig“ oder „kritisch“?**
  Die Klasse bestimmt, ob eure Selbstbewertung reicht oder eine benannte Stelle prüfen muss.
  `Frist 12/2027` `Zuständig: Kanzlei, Intern`

- [ ] 3 **Wird euer Produkt mit sicheren Standardeinstellungen ausgeliefert – individuelle Passwörter statt „0000“, Datenfreigaben per Opt-in?**
  Secure by Default ist ein Design-Thema: Sicherheit muss der Auslieferungszustand sein, nicht die Option.
  `Frist 12/2027` `Zuständig: Entwicklungspartner, Intern`

- [ ] 4 **Ist für jedes Produkt ein Supportzeitraum festgelegt und dokumentiert – und ist die Wartung eurer App über diese gesamte Zeit vertraglich gesichert?**
  Mindestens 5 Jahre kostenlose Sicherheitsupdates: Der Wartungsvertrag eurer App muss so lange tragen wie die Pflicht.
  `Frist 12/2027` `Zuständig: Intern`

02 Entwicklung

5 Punkte

- [ ] 5 **Erzeugt jeder App-Release automatisch eine SBOM, die auch native Ebenen und Vendor-SDKs umfasst?**
  Ohne aktuelle Software-Stückliste gibt es keine schnelle Antwort auf die Frage: „Sind wir von dieser CVE betroffen?“
  `Frist 12/2027` `Zuständig: Entwicklungspartner`

- [ ] 6 **Sind alle Datenwege verschlüsselt – auch die letzte Meile zwischen App und Gerät im lokalen Netz – und sensible Daten auf dem Telefon?**
  TLS zur Cloud reicht nicht, wenn App und Gerät im WLAN Klartext sprechen.
  `Frist 12/2027` `Zuständig: Entwicklungspartner` `[teils Hardware]`

☐ 7 **Liegen Tokens und Zugangsdaten im Keystore/Keychain statt im Klartext – mit Ablauf, Refresh und Widerruf?**

Der Klassiker in Bestands-Apps: unbegrenzt gültige Tokens im Klartext in den SharedPreferences.

Frist 12/2027 · Zuständig: Entwicklungspartner

☐ 8 **Ist der Release-Build frei von Debug-Resten – Test-Endpoints, Staging-URLs, Tokens in Logs, ungesicherte exportierte Komponenten?**

Der Block mit den schnellsten Erfolgen – vieles davon ist in Tagen behoben.

Frist 12/2027 · Zuständig: Entwicklungspartner

☐ 9 **Habt ihr für einkompilierte Dritt-SDKs Support-Zusagen der Lieferanten – und wisst ihr, welche Daten sie sammeln?**

Der CRA verpflichtet auch eure Zulieferkette. „Weil das SDK das halt macht" ist keine Antwort mehr.

Frist 12/2027 · Zuständig: Intern, Entwicklungspartner

03 Release & Dokumentation

4 Punkte

☐ 10 **Könntet ihr eure technische Dokumentation morgen einer Marktüberwachungsbehörde vorlegen – Risikobewertung, Maßnahmen, SBOM, Prozesse?**

Zum Großteil ein Nebenprodukt sauberer Arbeit: dokumentierte CI-Schritte, Architektur-Entscheidungen, Prozessbeschreibungen.

Frist 12/2027 · Zuständig: Intern, Kanzlei

☐ 11 **Ist geklärt, welches Konformitätsbewertungsverfahren für euch gilt und wer es wann durchführt?**

Bewertung und Erklärung bleiben Herstellerpflicht – auch wenn Agenturen und Berater zuarbeiten.

Frist 12/2027 · Zuständig: Kanzlei, Intern

☐ 12 **Ist der Weg zur CE-Kennzeichnung samt Konformitätserklärung geplant – mit dem CRA als neuem Bestandteil?**

Für viele Software-Anbieter ist es die erste CE-Kennzeichnung überhaupt – Vorlauf einplanen.

Frist 12/2027 · Zuständig: Kanzlei, Intern

☐ 13 **Liegen die vorgeschriebenen Nutzerinformationen vor – Supportzeitraum, Update-Verhalten, Meldekontakt, Hinweise zur sicheren Inbetriebnahme?**

Sie gehören zum Produkt wie die Bedienungsanleitung – und sind öffentlich sichtbar, also das Erste, was geprüft wird.

Frist 12/2027 · Zuständig: Intern, Kanzlei

04 Betrieb

4 Punkte

☐ 14 **Erfahrt ihr automatisch von neuen Schwachstellen in euren Abhängigkeiten – oder aus der Presse?**

SBOM gegen CVE-Feeds abgleichen (z. B. Dependency-Track) macht aus der Stückliste ein Frühwarnsystem.

Frist 12/2027 · Zuständig: Entwicklungspartner

☐ 15 **Könnt ihr jederzeit binnen weniger Tage einen Sicherheitspatch bauen, testen und in beide Stores bringen – mit vertraglich zugesagten Reaktionszeiten?**

Die Pflicht verlangt eine dauerhafte Fähigkeit, keinen Einmal-Zustand: Pipeline, Tests und Zuständigkeit müssen stehen, bevor der Ernstfall kommt.

Frist 12/2027 · Zuständig: Intern, Entwicklungspartner

☐ 16 **Wisst ihr, welche App- und Firmware-Versionen im Feld laufen – um im Ernstfall Betroffene in Stunden statt Tagen einzugrenzen?**

Die Kernfrage jeder Meldung lautet: Wie viele sind betroffen – und welche nicht?

Frist 09/2026 | Zuständig: Entwicklungspartner | [teils Hardware]

☐ 17 **Habt ihr faktischen Zugriff auf Quellcode, Signing-Keys und beide Store-Konten – unabhängig von jeder einzelnen Person oder Agentur?**

Fehlt eines davon, ist eure Update-Fähigkeit eine Hoffnung, keine Fähigkeit – die Pflicht bleibt trotzdem bei euch.

Frist 09/2026 | Zuständig: Intern

05 Meldewesen

3 Punkte

☐ 18 **Gibt es eine veröffentlichte, überwachte Kontaktstelle für Schwachstellenmeldungen – security@-Adresse plus security.txt, mit Vertretungsregelung?**

Sicherheitsforscher suchen zuerst nach der security.txt auf eurer Domain. Findet niemand einen Kanal, landet die Meldung woanders.

Frist 09/2026 | Zuständig: Intern

☐ 19 **Erreicht eine Schwachstellenmeldung, die Freitagabend eingeht, bis Samstagmittag eine entscheidungsbefugte Person – mit Meldeweg an CSIRT und ENISA im Playbook?**

Die 24-Stunden-Frist läuft ab Kenntnis – und richtet sich nicht nach Bürozeiten. Ein einseitiges Playbook mit Vertretung reicht; es muss nur existieren.

Frist 09/2026 | Zuständig: Intern, Kanzlei

☐ 20 **Könnt ihr betroffene Nutzer gezielt erreichen – Push oder In-App-Hinweis, mit E-Mail als Rückfallweg – inklusive konkreter Handlungsanweisungen?**

Die Meldung an die Behörde ist nur die halbe Pflicht: Auch Betroffene müssen informiert werden – über einen Kanal, der wirklich ankommt.

Frist 09/2026 | Zuständig: Entwicklungspartner, Intern

Auswertung

Zählt eure Häkchen zusammen – jedes „Nein“ oder „Weiß nicht“ ist ein Punkt für euer Maßnahmen-Backlog.

Viele offene Punkte
0–12 Häkchen

Erst das Gesamtbild, dann die Reihenfolge – dafür gibt es direkt darunter zwei Wege.

Einzelne offene Punkte
13–17 Häkchen

Nach Frist priorisieren: alles mit 09/2026 zuerst, der Rest nach Risiko in die normale Weiterentwicklung.

Starke Grundlage
18–20 Häkchen

Nächster Schritt: technische Dokumentation vervollständigen und die Konformitätsbewertung vorbereiten.

Zu viele offene Häkchen?

Der CRA-Readiness-Check macht aus dieser Checkliste einen priorisierten Maßnahmenkatalog an eurer echten App – in ca. 5 Werktagen, zum Festpreis:
flutterapps.agency/cyber-resilience-act/readiness-check

Direkt zum Readiness-Check