KILDE

CRA Reporting-Ready Pack — Edition 1.2

SRP-mechanics edition · current to 21 August 2026

General information and document templates only. Not legal advice; no compliance outcome is guaranteed. Licensed for single-organisation use — see the Licence at the end of this document. © 2026 Kilde.

START HERE — Are you in scope, and what do you owe on 11 September 2026?

CRA Reporting-Ready Pack · v1.0 · verified against sources dated 15 July 2026 · General information and implementation templates only. This is not legal advice and not a conformity assessment; no attorney-client relationship is created. Where the law is quoted, it is cited; some pinpoint paragraph numbers are being confirmed against the Official Journal before this pack quotes them verbatim (see the change tracker). For decisions about your specific product, involve counsel and, where required, a notified body — this pack makes those engagements shorter and cheaper.

The single thing to understand first: on 11 September 2026, only one part of the CRA switches on — the Article 14 reporting duty — but it switches on for products you have already sold. The heavy design and documentation requirements don't apply until 11 December 2027. This pack makes you able to file on time in September, and hands you the December-2027 folder structure to grow into.

Step 1 — Are you in scope? (15 minutes)

Q1. Is your thing a "product with digital elements"? That means software or hardware that connects — directly or indirectly — to a device or network. Downloadable software counts. Firmware counts. Connected hardware counts. - Pure cloud services / SaaS are generally governed by a different law (NIS2), not the CRA — with one catch: a cloud back-end counts as part of your product when your product can't function without it and you built it (or had it built). If your desktop/mobile/hardware product phones home to a service you operate, that service likely rides along. The draft Commission guidance addresses exactly this line; the pack's FAQ (file 08) walks the common cases. - → If you only sell a website or a pure SaaS with no distributed software or device, you are probably out of CRA scope. Document that conclusion (file 07) and stop here — but re-check if you ship a desktop app, mobile app, browser extension, firmware, or hardware.

Q2. Which role are you? (You can be more than one.) - Manufacturer — you develop it, or have it developed, and sell it under your own name or brand. White-labelling someone else's product under your brand makes you the manufacturer. Article 14 reporting is a manufacturer duty. - Importer — you're EU-established and you place a non-EU-branded product on the EU market. - Distributor — you make it available in the chain without being manufacturer or importer. - Open-source steward — a non-profit-style sustained supporter of commercial open source: lighter regime, and no administrative fines. → If you are a manufacturer, the reporting duty is yours — continue. Importers/distributors: your big duties are verification (covered in the optional importer/distributor annex), and you should know your manufacturers' reporting obligations because you'll be asked.

Q3. Are your products used in the EU? Placing on the EU market, or having EU users, puts you in scope wherever your company sits. A non-EU software or device maker with EU customers is a CRA manufacturer.

Q4. Do you have products already on the market (sold before 11 December 2027)? → Yes → the reporting duty still covers them from 11 September 2026. The law is explicit that Article 14 applies to in-scope products placed on the market before the December 2027 cutover. There is no "our existing products are grandfathered" position. This is the fact most teams get wrong.

Step 2 — What actually triggers a report? (know this cold before you need it)

Two things, and only two, start the clock (full detail + decision tree in file 02): 1. An actively exploited vulnerability in your product — meaning there is reliable evidence someone malicious has actually exploited it, not merely that it could be exploited. 2. A severe security incident affecting your product — one that harms (or could harm) the security of important data/functions, or that led (or could lead) to malicious code running in your product or your users' systems. When either happens, you owe: an early warning within 24 hours, a fuller notification within 72 hours, and a final report later (the exact final-report deadline differs between the two tracks — file 02 has both clocks). Reports go to a national coordinator authority (a "CSIRT") and the EU agency ENISA, through a central reporting platform.

Step 3 — Do these five things now (each has a file)

1. Finish scope + role and write it down — file 07 evidence log. (You just did most of it.)
2. Stand up the reporting runbook so a 24-hour clock never catches you improvising — file 02. This is the September deadline. Do it first.
3. Publish a coordinated vulnerability disclosure (CVD) policy + contact point — file 03. (Also a Dec-2027 requirement, but cheap to do now and it's where exploited-vuln reports will reach you.)
4. Decide and publish your support period + end-of-life policy — file 04.
5. Start the technical-documentation folder and an SBOM — files 05–06. These are December-2027 requirements; starting the folder now means it's not a panic later.

Step 4 — Two dates for your calendar

- 11 September 2026 — Article 14 reporting applies, including to products already sold. The reporting platform is expected to be live by then; if it slips, the duty to notify still stands and the runbook (file 02) covers the fallback.
- 11 December 2027 — the full essential requirements, technical documentation, CE marking, and conformity assessment apply. The pack's roadmap files get you started; the update tracker counts you down and folds in official templates and standards as they publish.

A note on penalties (so you can size the risk honestly)

Breaching the Article 14 reporting duty sits in the CRA's top penalty tier — the same tier as the essential requirements. For small companies, regulators must take company size into account when setting any fine, and open-source stewards can't be fined at all. Whether fines can attach to reporting breaches before the December 2027 full-application date is genuinely unsettled and depends on national implementing law — this pack flags it as an open question rather than guessing, and points you to your Member State's rules. The practical near-term pressure for most makers is the same as it is everywhere in this space: enterprise customers will ask for your CRA posture in procurement. The evidence log answers them.

File 01 — Obligations Timeline & Penalties (what bites when, and what it costs)

One-page reference. General information only; not legal advice. Dates/penalties verified against CELEX 32024R2847 (2026-07-15).

§1 · The timeline

Date	What switches on	Who it hits
10 Dec 2024	CRA entered into force (20 days after OJ publication 20 Nov 2024)	—
11 June 2026	Conformity-assessment-body / notified-body provisions (Chapter IV)	notified bodies
11 September 2026	Article 14 reporting duty — 24h/72h/final reports for actively-exploited vulnerabilities and severe incidents. Applies to products already on the market (Art 69(3)).	manufacturers — including of the installed base
11 December 2027	Full CRA: essential requirements (Annex I), technical documentation (Annex VII), CE marking, conformity assessment, support-period/EOL, importer/distributor verification duties	manufacturers, importers, distributors

The one thing teams get wrong: the September 2026 reporting duty is not limited to new products. Article 69(3) ("by way of derogation from paragraph 2…") extends Article 14 to in-scope products placed on the market before 11 December 2027 — i.e., your existing installed base. There is no grandfathering for reporting.

§2 · What "no grandfathering for reporting" means in practice

From 11 September 2026, if a product you've already sold has a vulnerability that is being actively exploited, or suffers a severe security incident, the 24-hour clock applies — even if that product shipped years ago and even though its design requirements don't bite until December 2027. That's why File 02 (the runbook) is the September priority, and the rest of the pack is the runway to December 2027.

§3 · Penalties (size the risk honestly)

Breach	Cap (whichever is HIGHER)	CRA basis
Essential requirements (Annex I) or Articles 13–14 (incl. the reporting duty)	€15,000,000 or 2.5% of worldwide annual turnover	Art 64(2)
Most other operator obligations	€10,000,000 or 2%	Art 64(3)