Cyber Resilience Act: can you still sell your products in the EU after 11 December 2027?

Be ready now to report an actively exploited vulnerability or severe incident in any product on the EU market within 24 hours. Before 11 December 2027, give every product a class, a support period, a risk assessment, an SBOM and technical documentation, so it can carry the CE marking.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**Companies that make, import or distribute hardware or software sold in the EU, and open-source stewards**

Latest version
sheets.einblick.dev/cra-product-makers/

If you only do five things

1. **Be able to report within 24 hours.**
   Reporting has applied since 11 September 2026, also to products placed on the market before December 2027 and after their support ends[3]. Name an owner and a deputy with EU Login accounts and MFA, and decide which CSIRT you report to[5].
2. **Classify each product by its core functionality.**
   Match it against Implementing Regulation (EU) 2025/2392[4]. Default products may always self-assess; important and critical ones may need a notified body[3].
3. **Set a support period per product.**
   Base it on expected use, comparable products and your components' own support, and make it at least 5 years unless use is shorter[1]. Show the end month and year at purchase[1].
4. **Write the risk assessment first.**
   It decides how each Annex I requirement applies and goes into the technical documentation[1]. Cover planned features too, so the updates that add them aren't substantial modifications[3].
5. **Run vulnerability handling as a process.**
   Due diligence on third-party and open-source components, an SBOM per release, a disclosure policy and contact, and free security updates[1]. The supply chain and secure development sheets show how.

Are you in scope, and in which role?

1. **Does it connect to a device or network?**
   If so, the CRA covers it, with the remote data processing it needs to work[1]. Web apps used only in a browser, websites and SaaS are not products themselves[3].
2. **Is it excluded?**
   Yes, if it's a medical or diagnostic device, a motor vehicle, a certified aviation product, marine equipment, an identical spare part or made only for national security or defense[1].
3. **Do you supply it commercially?**
   Charging for it or for support beyond cost, monetizing it through other services or requiring personal data for more than security and compatibility counts, even if it's free[1]. Open source you don't monetize doesn't[1].
4. **Are you an open-source steward?**
   You are if you're a foundation or company that systematically supports non-monetized open source meant for commercial use[3]. Stewards need a documented security policy[1], report from December 2027[5] and can't be fined[1].
5. **Which role do you have?**
   Manufacturers sell under their own name; importers and distributors check the CE marking and documents first[1]. Rebranding or substantially modifying a product makes you its manufacturer[1].

Product classes and conformity assessment

- **Default.** Anything whose core functionality isn't in Annex III or IV. Self-assessment (module A) is always allowed[3].
- **Important, class I.** 19 categories, such as identity and access management, browsers, password managers, antivirus, VPNs, operating systems, routers and smart home security products. Self-assess only by fully applying a cited harmonized standard, common specification or EU certificate at level substantial; otherwise use a notified body[1].
- **Important, class II.** Hypervisors, container runtimes, firewalls, intrusion detection and prevention systems and tamper-resistant chips. Always third party[1].
- **Critical.** Hardware security boxes, smart meter gateways and smartcards: EU certification where a delegated act requires it, otherwise as class II[1]. The class of the whole product counts, not that of its components[3].
- **Check which standards are cited.** Only standards cited in the Official Journal give presumption of conformity[1]. ETSI's approval of its 17 product-specific drafts ends between mid-September and mid-November 2026, by product[10].

Annex I in practice

- **No known exploitable flaws at release.** Known means in the EU vulnerability database or another prominent one, or reported to you[3].
- **Secure defaults.** A secure default configuration with a reset, access control, encryption of stored and transmitted data, minimal data and a way to delete it all[1].
- **Automatic security updates on by default, where applicable.** With an opt-out, notifications and a way to postpone. Not required for components or where users don't expect them, as in industrial networks[1].
- **An SBOM per release.** Machine-readable, covering at least top-level dependencies, and it needn't be public[1]. BSI TR-03183-2 asks for CycloneDX 1.6 or SPDX 3.0.1 or later, with dependencies resolved through everything you ship[8].
- **One contact point, not just a chatbot.** A single point of contact not limited to automated tools, plus a disclosure policy[1]. BSI's voluntary TR-03183-3 adds a signed `security.txt`[9].
- **Free fixes, kept available.** Keep each security update available for 10 years or the rest of the support period, if longer[1]. For software, fixing only the latest version is fine if upgrading costs users nothing extra[1].
- **Advisories and upstream reports.** Publish fixed flaws, in CSAF as the BSI recommends[1,9], and send component flaws to their maintainer[1].

Reporting clocks since 11 September 2026

Clocks start at reasonable certainty after a prompt first check[3]. Report once on ENISA's platform, in Germany to CERT-Bund, and tell affected users[1,6].

Actively exploited vulnerability

Reliable evidence of exploitation[1]; a public exploit isn't enough[6].

24 hours	72 hours	Fix + 14 days
Early warning	Notification	Final report

Severe incident

It harms or could harm the product's protection of sensitive or important data or functions, or could plant malicious code in it or users' systems[1]. Ransomware at the maker counts only if it could affect the product, its updates or signing keys[6].

24 hours	72 hours	1 month later
Early warning	Notification	Final report

Documentation, CE marking and fines

- **Technical documentation (Annex VII).** Architecture, vulnerability handling with SBOM and disclosure policy, risk assessment, support period reasons, standards, test reports and the declaration. Keep it 10 years or for the support period, if longer[1].
- **EU declaration of conformity.** Follow Annex V, ship it or a simplified version with its web address, and issue one for all EU acts that need one[1].
- **CE marking from 11 December 2027.** On the product, or the packaging and declaration; for software, on the declaration or its website[1].
- **Fines up to €15 million or 2.5% of worldwide turnover.** For breaching Annex I or Articles 13 and 14; €10 million or 2% for most other duties. Micro and small manufacturers aren't fined for a late 24-hour early warning, under Article 64(10) as corrected in July 2025[1,2].

What you can skip

- **Waiting for harmonized standards.** The risk assessment, SBOM, disclosure policy and update channel don't depend on them.
- **Reporting every vulnerable dependency.** Flaws that aren't reachable or exploited in your product aren't reportable; tell the maintainer[3].
- **Redesigning products that already hold up.** Designs from before the CRA need no change if the risk assessment shows adequate measures[3].
- **Registering on ENISA's platform early.** ENISA advises registering only when you first need to report[5].

Mistakes that cost the most

- **Counting on the transition for hardware.** Every unit placed on the market from 11 December 2027 must comply, even of an older model[3].
- **Picking the wrong CSIRT.** The notification may be invalidated and need resubmitting[5].
- **Rebranding without noticing.** An importer or distributor selling under its own name becomes the manufacturer[1].
- **A 5-year support period by reflex.** The Commission says 5 years is not a default; products used longer need longer support[3].

What changed in 2026

- **Reporting went live on 11 September.** ENISA's platform is English only, has no API yet, and its 72-hour counter can show reports overdue early[5].
- **Draft Commission guidance, 27 July.** It explains scope, open source, substantial modification and support periods, and isn't binding[3].
- **Germany is naming the BSI.** A bill the Bundestag passed on 15 October would make it market surveillance authority[11,12].
- **Radio equipment moves to the CRA.** The radio equipment cybersecurity delegated act is repealed from 11 December 2027[13].

What this looks like at your size

Small team, no security staff

- List every product and version you sell in the EU, with its class and support end date.
- Write a one-page runbook: who reports, to which CSIRT, from which EU Login accounts.
- Work through BSI TR-03183-1 as a checklist[7].

Growing, with IT or security staff

- Name a product security owner and ship an SBOM and advisories with every release.
- Plan for a notified body now if a product needs one; Member States aim to have enough by 11 December 2026[1].
- Document one product end to end, then reuse it for its variants[3].

Enterprise or regulated

- Build module H on your ISO/IEC 27001 ISMS, as BSI TR-03183-H shows[7].
- Run CRA reports in your NIS2 incident process; the EU security laws sheet has those clocks.
- Agree how importers and distributors pass on the vulnerabilities they must report to you[1].

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which confirmed the small-maker fines exemption in the July 2025 corrigendum, added component due diligence, a non-public SBOM and the Bundestag's 15 October vote, and separated BSI recommendations from CRA duties.

Sources

1. Regulation (EU) 2024/2847 (Cyber Resilience Act). EUR-Lex, 2024. eur-lex.europa.eu
2. Corrigendum to Regulation (EU) 2024/2847, Article 64(10). EUR-Lex, 2 Jul 2025. eur-lex.europa.eu
3. Draft Commission guidance on the application of the CRA, annex to C(2026) 5252. European Commission, 27 Jul 2026. ec.europa.eu
4. Implementing Regulation (EU) 2025/2392 (important and critical products). EUR-Lex, 28 Nov 2025. eur-lex.europa.eu
5. CRA Single Reporting Platform: FAQ. ENISA, updated 15 Oct 2026. enisa.europa.eu
6. CRA Single Reporting Platform. BSI, checked 5 Nov 2026. bsi.bund.de
7. TR-03183: Cyber Resilience Requirements. BSI, checked 5 Nov 2026. bsi.bund.de
8. TR-03183-2: Software Bill of Materials, v2.1.0. BSI, 20 Aug 2025. bsi.bund.de
9. TR-03183-3: Vulnerability Reports and Notifications, v1.0.0. BSI, 20 Aug 2025. bsi.bund.de
10. ETSI launches approval process for 17 European Standards supporting the Cyber Resilience Act. ETSI, 13 Aug 2026. etsi.org
11. Ausschuss billigt Gesetzentwurf zu Cyberresilienz-Verordnung. Deutscher Bundestag, 14 Oct 2026. bundestag.de
12. Gesetzesbeschluss zur Cyberresilienz-Verordnung, Drucksache 621/26. Bundesrat, 30 Oct 2026. dserver.bundestag.de
13. Delegated Regulation (EU) 2026/339 repealing Delegated Regulation (EU) 2022/30. EUR-Lex, 29 Apr 2026. eur-lex.europa.eu