What does the EU Cyber Resilience Act mean for PostgreSQL and its community?

Peter Eisentraut

October 2026

peter@eisentraut.org
https://peter.eisentraut.org/
@petereisentraut@mastodon.social

peter.eisentraut@enterprisedb.com
https://www.enterprisedb.com/
@edbpostgres@mastodon.social

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

Applies to

"products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network"

(CRA Art. 2)

What about non-EU?

Exceptions

- medical devices
- motor vehicles
- civil aviation products
- marine equipment
- spare parts
- products exclusively for defence purposes
- products specifically for processing classified information

Further exceptions

- trade fairs, exhibitions, demonstrations (with marking)
- unfinished software for testing purposes (with marking)

“important” and “critical” products

- important, e.g.:
  - browsers
  - password managers
  - operating systems
  - network management systems
- critical, e.g.:
  - hypervisors
  - firewalls

⇒ does not affect PostgreSQL

Important dates

- entered into force on 10 December 2024
- applies from 11 December 2027
- reporting obligations of manufacturers (Art. 14) from 11 September 2026
- notification of conformity assessment bodies (Chap. IV) from 11 June 2026

Agencies and institutions

- in each member state:
  - market surveillance authority (🔗list)
  - CSIRT designated as coordinator (🔗list)
  - notifying authority (🔗list)
- ENISA 🇪🇺

Relationship with other EU laws

- Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847): government regulation of PDE placed on the market
- Product Liability Directive (PLD) update (Directive (EU) 2024/2853): extends/clarifies product liability to software
- 2nd Network and Information Security directive (NIS2) (Directive (EU) 2022/2555): cybersecurity for (critical) infrastructure
- Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554): cybersecurity for financial sector

Roles & obligations

- (commercial) manufacturer: many obligations
- open-source software steward: some obligations
- everyone else: no obligations

“Manufacturer”?

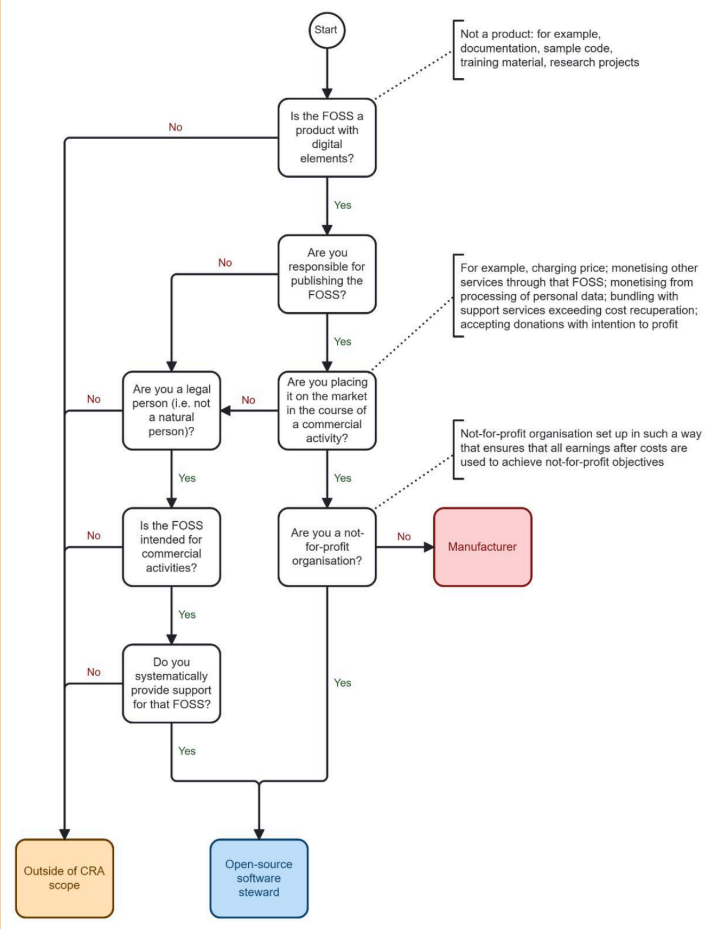
“a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge”

(CRA Art. 3)

“Open-source software steward”

“a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products”

(CRA Art. 3)



(Source: Commission guidance on the application of the Cyber Resilience Act (CRA))

Manufacturer/steward examples

company that sells PostgreSQL or variants with support	manufacturer
company that sells (only) training or consulting for PostgreSQL	neither
company that sells PostgreSQL DBaaS	neither
company that does not sell any services around PostgreSQL but develops an open source software for internal use and also offers it for download	steward
Cloud Native Computing Foundation → Linux Foundation	steward
PostgreSQL Europe association	steward (?!?)
Software in the Public Interest (SPI)	steward
PostgreSQL Core Team	neither
PostgreSQL Security Team	neither
individual PostgreSQL hacker	neither

Obligations of manufacturers

(excerpt; CRA Art. 13)

- product complies with essential cybersecurity requirements
- risk assessment (kept up to date)
- due diligence when integrating components sourced from third parties
- report vulnerabilities in integrated components to manufacturers or maintainers, share modifications
- vulnerabilities are handled
- at least 5 years of security support
- (can be limited to latest version, if upgrades are easy)
- security updates available for at least 10 years
- single point of contact for reporting vulnerabilities
- conformity assessment and declaration
- technical documentation

Essential cybersecurity requirements

(excerpt; CRA Annex I Part I)

- made available on the market without known exploitable vulnerabilities
- made available on the market with a secure by default configuration
- ensure protection from unauthorised access by appropriate control mechanisms
- protect the confidentiality of stored … data
- resilience and mitigation measures against denial-of-service attacks
- provide security related information by recording … activity

⇒ harmonised standards

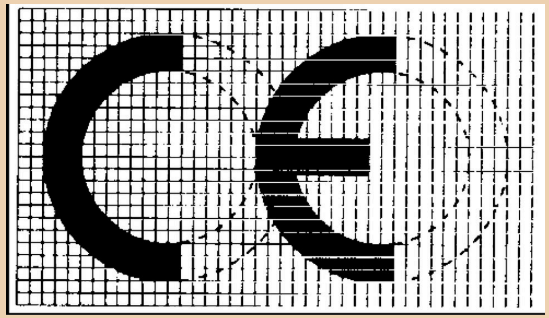
Vulnerability handling requirements

(excerpt; CRA Annex I Part II)

- drawing up a software bill of materials (SBOM) in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products
- where technically feasible, new security updates shall be provided separately from functionality updates
- apply effective and regular tests and reviews of the security of the product with digital elements
- put in place and enforce a policy on coordinated vulnerability disclosure

Conformity assessment and declaration

- either self-assessment or assessment by certified body
- include conformity declaration (or on website)
- affix CE marking



Reporting obligations of manufacturers

(excerpt; CRA Art. 14)

- report actively exploited vulnerabilities
- report severe security incidents
- inform the impacted users

(24h)

from 11 September 2026!

⇒ single reporting platform (SRP) (🔗 link)

Voluntary reporting

(CRA Art. 15)

- everyone can report vulnerabilities, “cyber threats” or security incidents to CSIRT or ENISA
- manufacturers are informed
- no additional obligations upon reporter

Obligations of open-source software stewards

(CRA Art. 24)

- put in place “cybersecurity policy”
- cooperate with the market surveillance authorities
- reporting obligations like manufacturers (Art. 14)
    - if involved in the development
    - if providing infrastructure
- no administrative fines against open-source software stewards (Art. 64(10))

Security attestation of free and open-source software

“In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation.”

(CRA Art. 25)

Tips for open-source maintainers

to support due diligence and work toward attestations

- Authorship: clearly identify maintainers
- Governance: documentation, contribution guideline
- Licensing: license clearly identified; open-source license for all components, artifacts, and all dependencies
- Quality: identify third-party dependencies, public source code and change history, vulnerability reporting guide, repeatable testing procedures, memory safety mitigations, more than one contributor, change review required
- Build and Release: build instructions, version numbering, secure asset distribution, release notes
- Vulnerability Management: identify security contact, timely handling of vulnerabilities
- End-of-Life: clearly communicate discontinuation of support

based on

- https://github.com/orcwg/cra-attestations/blob/main/proposals/template-lite.md
- OpenSSF CRA Readiness Guide for Maintainers and Developers

Invitation to collaborate

Friday, 09:00 – 12:00, Room Audit 3B

“A Postgres Ecosystem Foundation?”

https://2026.pgconf.eu/community-events/postgres_ecosystem_foundation/

Homework for manufacturers

- clarify your roles (manufacturer etc.)
- analyze own software and dependencies
- prepare/follow reporting obligations
- document everything

Links

- EU
    - Cyber Resilience Act (EUR-Lex)
    - Cyber Resilience Act - Implementation (EU)
    - Commission guidance on the application of the Cyber Resilience Act (CRA)
- member states' MSAs and CSIRTs
    - (see lists earlier)
- information for open source work
    - OpenSSF
    - ORC WG
- training courses
    - Eclipse Foundation
    - Linux Foundation

Bye / Questions / Contact

peter@eisentraut.org
https://peter.eisentraut.org/
@petereisentraut@mastodon.social

peter.eisentraut@enterprisedb.com
https://www.enterprisedb.com/
@edbpostgres@mastodon.social