Was bedeutet der EU Cyber Resilience Act für PostgreSQL und seine Anwender?

Peter Eisentraut

April 2026

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

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

Was bedeutet die EU Cyberresilienz-Verordnung für PostgreSQL und seine Anwender?

Peter Eisentraut

April 2026

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

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

Gilt für

„auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“

(CRV Art. 2)

Ausnahmen

- Medizinprodukte
- Kraftfahrzeuge
- Luftfahrttechnische Erzeugnisse u. a.
- Schiffsausrüstung
- Ersatzteile
- Produkte ausschließlich für Verteidigungszwecke
- Produkte speziell für die Verarbeitung von Verschlusssachen

Weitere Ausnahmen

- Messen, Ausstellungen, Vorführungen (mit Kennzeichnung)
- unfertige Software für Testzwecke (mit Kennzeichnung)

„wichtige“ und „kritische“ Produkte

- wichtig, z. B.:
  - Browser
  - Passwort-Manager
  - Betriebssysteme
  - Netzwerkmanagementsysteme
- kritisch, z. B.:
  - Hypervisoren
  - Firewalls

⇒ betrifft PostgreSQL nicht

Wichtige Daten

- trat in Kraft am 10. Dezember 2024
- gilt ab 11. Dezember 2027
- Meldepflichten der Hersteller (Art. 14)
  ab 11. September 2026
- Notifizierung von Konformitätsbewertungsstellen
  (Kap. IV) ab 11. Juni 2026

Behörden und Einrichtungen

- Marktüberwachungsbehörde (🇩🇪 BSI, 🇦🇹 Bundesamt für Cybersicherheit)
- notifizierende Behörde (🇩🇪 BSI, 🇦🇹 Bundeskanzleramt)
- als Koordinator benanntes CSIRT (🇩🇪 BSI)
- ENISA 🇪🇺

„Hersteller“?

„eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich“

(CRV Art. 3)

„Verwalter quelloffener Software“

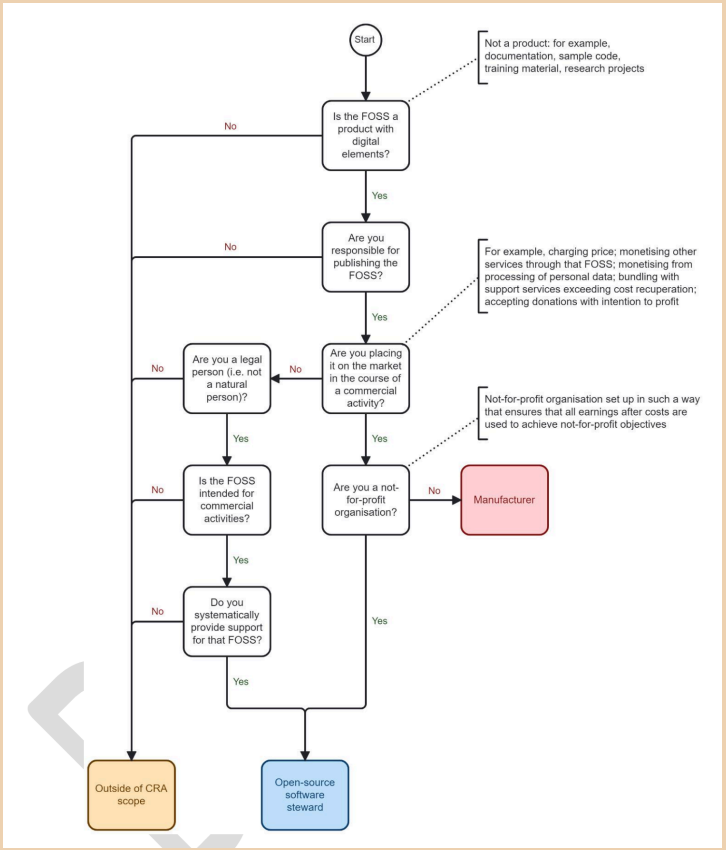
(open-source software steward)

„eine juristische Person, bei der es sich nicht um einen Hersteller handelt, die den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt“

(CRV Art. 3)

Hersteller/Verwalter Beispiele

Unternehmen, das PostgreSQL oder Varianten anbietet und mit Support verkauft	Hersteller
Unternehmen, das (nur) Schulungen und Beratung zu PostgreSQL verkauft	weder noch
Unternehmen, das PostgreSQL DBaaS verkauft	weder noch
Unternehmen, das keine Dienstleistungen zu PostgreSQL verkauft, aber eine Open-Source-Software für intern entwickelt und zum Herunterladen anbietet	Verwalter
Cloud Native Computing Foundation → Linux Foundation	Verwalter
PostgreSQL Europe association	Verwalter (?!?)
PostgreSQL Core Team	weder noch
PostgreSQL Security Team	weder noch
einzelner PostgreSQL Hacker	weder noch



(Quelle: Draft Commission guidance on the Cyber Resilience Act)

Pflichten der Hersteller

(Auszug; CRV Art. 13)

- Produkt entspricht grundlegenden Cybersicherheitsanforderungen
- Risikobewertung (fortlaufend aktualisiert)
- gebotene Sorgfalt walten lassen, wenn von Dritten bezogene Komponenten integriert werden
- Schwachstellen in integrierten Komponenten an Hersteller oder Maintainer melden, Änderungen teilen
- Schwachstellen werden behandelt
- mindestens 5 Jahre Unterstützung
- (kann auf letzte Version beschränkt werden, wenn Upgrades problemlos sind)
- Sicherheitsaktualisierungen mind. 10 Jahre verfügbar
- zentrale Anlaufstelle für Meldung von Schwachstellen
- Konformitätsbewertung und -erklärung
- technische Dokumentation

Grundlegende Cybersicherheitsanforderungen

(Auszug; CRV Anh. I Teil I)

- ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt
- mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt
- durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten
- Vertraulichkeit gespeicherter … Daten schützen
- Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server
- sicherheitsbezogene Informationen durch Aufzeichnung … bereitstellen

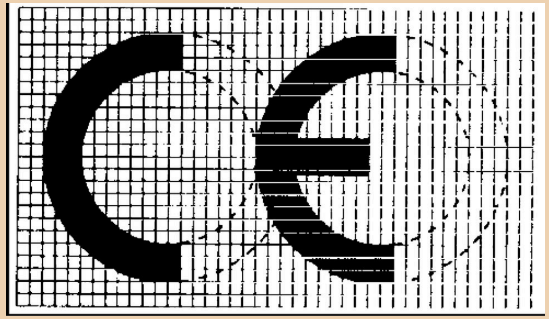
Anforderungen an die Behandlung von Schwachstellen

(Auszug; CRV Anh. I Teil II)

- Erstellung einer Software-Stückliste [SBOM] in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen
- soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden
- Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen
- eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen

Konformitätsbewertung und -erklärung

- Bewertung entweder selber oder von zertifizierten Stellen
- Konformitätserklärung beilegen (oder auf Website)
- CE-Zeichen anbringen



Meldepflichten der Hersteller

(Auszug; CRV Art. 14)

- aktiv ausgenutzte Schwachstellen melden
- schwerwiegende Sicherheitsvorfälle melden
- betroffene Nutzer informieren

(24h)

ab 11. September 2026!

Freiwillige Meldungen

(CRV Art. 15)

- jeder kann Schwachstellen, „Cyberbedrohungen“ oder Sicherheitsvorfälle an CSIRT oder ENISA melden
- Hersteller werden unterrichtet
- keine weiteren Pflichten für den Melder

Pflichten der Verwalter quelloffener Software

(CRV Art. 24)

- „Cybersicherheitsstrategie“ entwickeln
- mit Marktüberwachungsbehörden zusammenarbeiten
- Meldepflichten wie Hersteller (Art. 14)
  - wenn an der Entwicklung beteiligt
  - wenn Infrastruktur bereitgestellt wird
- keine Geldbußen gegen Verwalter quelloffener Software (Art. 64 Abs. 10)

Sicherheitsbescheinigung für freie und quelloffene Software

(Security attestation for free and open-source software)

„Um die in Artikel 13 Absatz 5 festgelegte Sorgfaltspflicht zu erleichtern, insbesondere in Bezug auf Hersteller, die freie und quelloffene Softwarekomponenten in ihre Produkte mit digitalen Elementen integrieren, wird der Kommission die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zu erlassen, um diese Verordnung durch die Einführung freiwilliger Programme zur Bescheinigung der Sicherheit zu ergänzen, die es den Entwicklern oder Nutzern von Produkten mit digitalen Elementen, die als freie und quelloffene Software gelten, sowie anderen Dritten ermöglichen, die Konformität dieser Produkte mit allen oder bestimmten grundlegenden Cybersicherheitsanforderungen oder sonstigen in dieser Verordnung festgelegten Verpflichtungen zu bewerten.“

(CRV Art. 25)

Hausaufgaben für Hersteller

(für die kommenden 6 Monate)

- eigene Software-Abhängigkeiten analysieren
- Rollen (Hersteller usw.) klären
- Meldepflichten vorbereiten
- Standardisierung weiter beobachten

Hausaufgaben für PostgreSQL-Projekt

(Zuarbeit für Hersteller)

- Schwachstellenbehandlung formalisieren
- für sekundäre Projekte: Unterstützungszeiträume, Sicherheitskonzepte, Meldestellen
- Checklisten für Cybersicherheitsanforderungen

Links

- Cyberresilienz-Verordnung (EUR-Lex)
- Cyber Resilience Act - Implementation (EU)
- Cyber Resilience Act (BSI)
- Draft Commission guidance on the Cyber Resilience Act

Tschüss / Fragen / Kontakt

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

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