OpenSSF
OPEN SOURCE SECURITY FOUNDATION

EU CYBER RESILIENCE ACT (CRA)

Key Dates:

- **EIF**: CRA law entered into force on December 10, 2024, as Regulation (EU) 2024/2847.
- **Mandatory**: Some requirements apply starting September 11, 2026.
- **Fully Enforced**: All requirements and obligations to be enforced by December 11, 2027 after which all products with digital elements (including software and remote data processing) must comply.

Who's Who: Manufacturer vs. Steward

- **Manufacturer**: Any person or company selling a Product with Digital Elements (PDE) in the EU must ensure compliance, conformance assessments, vulnerability management, incident reporting, free security updates (≥ 5 yrs).

- **Steward**: A "legal person…other than a manufacturer" that provides sustained, non-commercial support for FOSS PDEs; fewer obligations but must handle vulnerabilities and incidents.

Your Business Must…

- **Assess & Conform:** Classify your PDEs (Important, Critical, Default) and complete internal or external conformance checks.
- **Document & Report:** Produce technical docs (SBOMs, architecture, design), perform supply-chain risk assessments, and notify EU bodies of incidents/vulnerabilities within 24 hrs.
- **Manage Vulnerabilities:** Ensure releases ship without known exploitable flaws; establish processes for patching and updates

Essential Resources - Scan to Access

- **OpenSSF Global Cyber Policy WG**: Slack ▪ GitHub ▪ Mailing List
- **Free Course**: Understanding the EU CRA (LFEL1001).
- **Developer-focused blogs**: Practical guidance at your fingertips.
- **Open Source Security Project Baseline**: Actionable guidance to help meet CRA obligations.

HOW TO PARTICIPATE IN THE OPENSSF

openssf.org
github.com/ossf
openssf.slack.com
linkedin.com/company/openssf

EU CYBER RESILIENCE ACT

openssf.org/public-policy/eu-cyber-resilience-act/