WHAT YOU NEED TO KNOW ABOUT THE CYBER RESILIENCE ACT

EU's New Regulation Making Digital Products Safer and More Secure

What Is the CRA?

A new EU law (Regulation 2024/2847) that sets mandatory cybersecurity requirements for all products with digital elements - hardware and software - sold in the EU.

Who Must Comply?

- Manufacturers (inside and outside the EU)
- Software developers (including open-source if used commercially)
- Importers and distributors
- SMEs (with some simplified support)

What Does It Require?

- Cybersecurity by design and by default
- Regular security updates
- Transparent support period disclosure
- Secure vulnerability reporting & incident handling
- Clear CE marking to show compliance
- Conformity assessments based on risk level

Key Dates

- ✓ **November 20, 2024** Regulation published
- ✓ **December 10, 2024** CRA enters into force
- **September 11, 2026** Reporting obligations begin
- **December 11, 2027** Full compliance required

Penalties

- Up to €15 million or 2.5% of global annual turnover
- Product bans or recalls
- Public disclosure of violations

What Products are Covered?

- Smart devices (IoT, wearables, home tech)
- Software (apps, SaaS, operating systems)
- Connected industrial equipment
- Embedded systems in vehicles, healthcare, energy, etc.

How Consumers Benefit?

- Safer digital products
- Guaranteed update timelines
- Clear product info
- Reduced risk of cyberattacks

How to Prepare?

- Start CRA gap assessments now
- Implement vulnerability management
- Plan for secure lifecycle processes
- Ensure supplier compliance and documentation
- Monitor ENISA guidelines and standards

CRACoWi

www.cracowi.eu