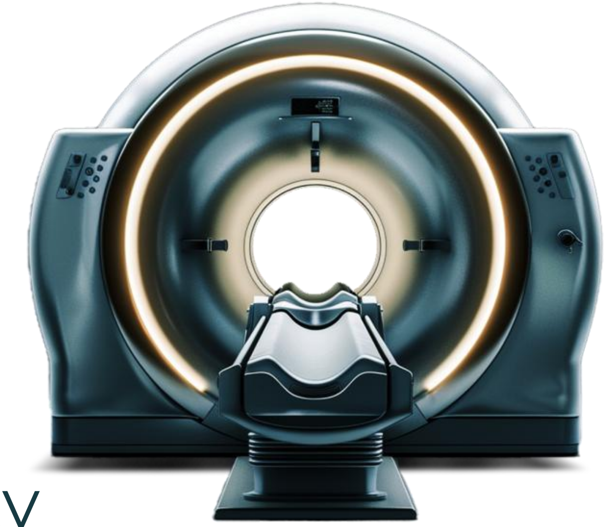
# A Checklist for EU RED (EN 18031) Compliance

1. Map your device connectivity (Wi-Fi, BLE, cellular)
2. Review product scope under RED vs MDR
3. Apply EN 18031-series standards
4. Create a security-by-design process
5. Build technical documentation for CE conformity
6. Set up a vulnerability handling process and disclosure policy



# 1. Map Your Device Connectivity

**Why it matters:**
RED applies specifically to radio equipment, meaning any device with a wireless interface (Wi-Fi, Bluetooth, cellular, etc.).

- ❑ Document every radio interface used in the device.
- ❑ Include hidden or low-energy components (e.g., BLE beacons).
- ❑ Map communication paths between modules and external systems.

# 2. Review Product Scope Under RED and MDR

## Why it matters:

Medical devices are typically regulated under the Medical Device Regulation (MDR), but if they include wireless communication, RED may also apply.

❑ Identify whether your device is strictly medical (under MDR) or also falls under RED due to connectivity.

❑ Devices not classified as “medical”, such as remote patient monitors, are likely fully RED-regulated.

❑ Understand overlapping obligations if both apply.

# 3. Apply EN 18031-series Standards

## Why it matters:

The EN 18031-series Standards will become mandatory in August 2025.

- ❑ Start implementing cybersecurity measures aligned for:
  - ❑ EN 18031-1: General principles
  - ❑ EN 18031-2: Risk assessment and threat analysis
  - ❑ EN 18031-3: Security requirements by class of device
- ❑ Conduct structured threat modeling and risk classification based on these guidelines.

# 4. Create a Security-by-Design Process

## Why it matters:

RED mandates proactive security - not just afterthought patching.

- □ Embed security into product development, from premarket to postmarket.
- □ Use secure coding and static code analysis.
- □ Define and implement access controls, secure boot, encryption, and update validation mechanisms.
- □ Train engineering teams on secure SDLC practices.

# 5. Build Technical Documentation for CE Conformity

**Why it matters:**

To apply the CE mark under RED, manufacturers must provide a Declaration of Conformity (DoC) and supporting technical files.

- ❑ Document your threat modeling, risk analysis, and implemented controls.
- ❑ Provide results from testing (e.g., penetration testing, vulnerability scans).
- ❑ Include your EN 18031 compliance mapping.
- ❑ Maintain this documentation for inspection by Notified Bodies or market surveillance.

# 6. Set Up Vulnerability Handling Process and Disclosure Policy

## Why it matters:

RED requires postmarket protection of devices, not just secure design (premarket).

- ❑ Establish a coordinated vulnerability disclosure policy.
- ❑ Monitor for new CVEs and zero-days affecting your components.
- ❑ Monitor, prioritize, and mitigate vulnerabilities in a timely and traceable manner.
- ❑ Inform customers and regulators if critical vulnerabilities are found.

# Product Security Partner of Choice

Gartner Names C2A Security to the 2024 Hype Cycle™ for Cyber-Physical Systems Security

> At Elekta, we’re committed to providing safe, resilient solutions to our customers. Our collaboration with C2A Security will enable us to integrate cybersecurity throughout our product portfolio, helping us meet compliance requirements while keeping our systems secure.

**John Chenoweth**
Chief Product Security Officer
Elekta

# Schedule a Demo Today