SE

EMBEDDED SYSTEMS ENGINEERING

SCHMITT CONSULTING S.A.R.L. · SC-SARL.COM

CRA Quick Check for Device Manufacturers

The new EU law on the cyber security of connected products — what has to be in place by September 2026, in plain language.

First binding deadline: 11 September 2026

Not 2027. Those who fail to prepare now will run out of time.

1 What it is about

The **Cyber Resilience Act** — **CRA** for short — has been in force since December 2024. It sets out how secure connected products must be against attacks from the internet. It affects everything that contains software or connects to a network: from the smart thermostat to industrial controllers to the app.

Many manufacturers believe they have until the end of 2027. That is true only for part of the obligations. The **first binding deadline is already in September 2026** — and it also applies to products that have long been on the market and are still being maintained.

11 September 2026

Reporting obligation. If a vulnerability is demonstrably exploited by attackers, this must be reported to the authorities **within 24 hours**.

11 December 2027

All remaining obligations. Product secure by design, security updates throughout its lifetime, a complete software bill of materials, formal assessment and CE marking.

The possible fines reach up to **15 million euros or 2.5 % of worldwide annual turnover** — whichever is higher. And: the law expressly applies to small manufacturers and sole providers too, not only to large corporations.

2 The key terms — briefly explained

Firmware
The control software built permanently into a device that makes it work in the first place — for example the program code in a machine, a sensor or a controller.

Vulnerability (security flaw)
A bug or weakness in the software through which an attacker can intrude into the device or manipulate it.

Software bill of materials (SBOM)
A complete list of all software components of a product — comparable to the parts list of a component, only for the program code. Without it you cannot tell whether the product is affected by a known vulnerability.

ENISA / CSIRT
ENISA is the EU cybersecurity agency, the central body for IT security in Europe. CSIRTs are the national state-run “computer fire brigades” that coordinate during security incidents. The 24-hour report goes to them.

Functional safety
Protecting a device against technical *malfunctions and failures* — established practice in automotive engineering, for instance. The CRA adds protection against *deliberate attacks*.

CE marking
The familiar CE mark on products. It confirms that a product meets the EU requirements and may be sold on the European market.

3 Are you CRA-ready? The checklist

Work through the following points. Every box you **cannot** tick with a clear conscience is unfinished work to be completed by September 2026.

OVERVIEW & ORGANISATION

- ☐ We know which of our products fall under the law.
- ☐ We know which older products we still maintain (and that are therefore affected as well).
- ☐ There is a person responsible for the CRA topic within the company.

SOFTWARE BILL OF MATERIALS

- ☐ For every product there is a complete list of all software components built in.
- ☐ We can also identify outdated components in it that the supplier no longer maintains.
- ☐ This list is kept continuously up to date, not created just once.

REPORTING PROCESS (MANDATORY FROM 09/2026)

- ☐ It is defined who notices an exploited vulnerability.
- ☐ It is defined who assesses it and who reports it.
- ☐ We can actually meet the 24-hour deadline organisationally — including at weekends.

TECHNICAL PROTECTION OF THE DEVICE

- ☐ The software in the device is stored encrypted and cannot simply be read out.
- ☐ Updates are tamper-proof — nobody can inject software that was slipped in.
- ☐ The device can receive security updates throughout its entire lifetime.
- ☐ On start-up the device checks that only genuine, unaltered software is running.

EVIDENCE & DOCUMENTATION

- ☐ We can demonstrate that development followed recognised programming standards.
- ☐ Reliability and attack resistance are thought of in one common concept, not separately.
- ☐ The documents needed for the later conformity assessment are kept from the very start.

4 How to proceed

The coming months will decide whether an orderly process is in place by September 2026 or whether things have to be improvised hectically. Those who start early spread the work — and avoid expensive last-minute fixes just before the deadline. The greatest leverage usually lies not in the technology alone, but in the clean interplay of the bill of materials, the reporting process and device protection.

→ Going deeper & support

You don't just want to grasp the requirements but to implement them? Three ways:

Technical books & software

Practical knowledge from over 35 years of embedded development — the technical foundation behind the CRA requirements. Available at **sc-sarl.com/en/produkte.html**

Free with it: “Formula Reference for Computer Scientists and Engineers”

Interactive HTML formula reference, 56 chapters, bilingual DE/EN, usable offline — free in the download area.

Personal support

From the software bill of materials to firmware hardening. Consultation at **sc-sarl.com/en/kontakt.html**

To the products & downloads →