

CRA reporting obligations

What your business needs to know before 11 September 2026

The Cyber Resilience Act (Regulation (EU) 2024/2847, CRA) adds a further layer of EU cybersecurity obligations, on top of the duties many businesses already face under NIS2, DORA and the GDPR.

It applies to products with digital elements – hardware and software that connect to a device or network.

The first obligations apply from 11 September 2026, when manufacturers must begin reporting actively exploited vulnerabilities and severe incidents. The remaining requirements apply from 11 December 2027.

WHO IS CAUGHT

- The obligations fall on manufacturers of products with digital elements. Manufacturer status does not depend on who built the product: a business placing a product on the market under its own brand takes on the obligations, even if a third party built it.
- The test is whether the product's intended purpose or reasonably foreseeable use includes a direct or indirect data connection to a device or network. A connection through another device is enough, as is one the manufacturer never intended but which is reasonably foreseeable.



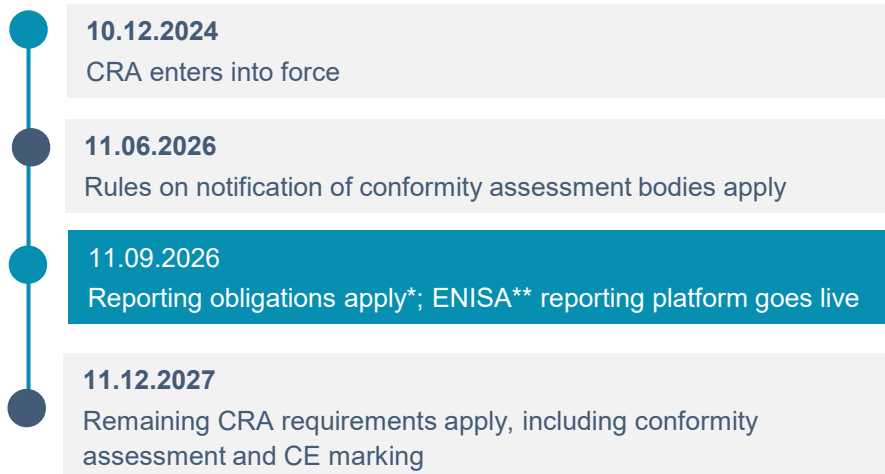
* Examples only. The list is illustrative and not exhaustive.

- The reporting obligations are the exception to the general timeline. They start to apply from 11 September 2026 and cover products already on the market, regardless of when they were placed on the market and of whether the manufacturer still supports them.
- What triggers the CRA reporting obligation is knowledge, not the existence of a problem. There is no duty to search the historic portfolio, but a customer complaint, a distributor notification or a media report starts the clock in the same way.
- A first useful exercise is confirming whether the business is deemed a manufacturer of each product, and who decides internally that an event is reportable.

CRA reporting obligations

What your business needs to know
before 11 September 2026

KEY DATES



* Reporting applies to all in-scope products, including those placed on the market before 11 December 2027

** ENISA is the European Union Agency for Cybersecurity

WHAT MUST BE REPORTED

Only two categories of events trigger the reporting obligation. The existence of a vulnerability, however serious, is not enough on its own.

**ACTIVELY EXPLOITED
VULNERABILITY –**
reliable evidence that a vulnerability in
the product has been exploited by a
malicious actor

*The clock starts only once there is reliable
evidence of active exploitation*



**SEVERE INCIDENT AFFECTING
PRODUCT SECURITY –**

an event affecting the product's ability to
protect data, or introducing malicious code
into the product or its users' systems



CRA reporting obligations

What your business needs to know before 11 September 2026

THE REPORTING CLOCK

Deadlines run from the point at which the manufacturer becomes aware of the event. Reports are submitted once, through a single platform operated by ENISA. Manufacturers must also inform affected users.



ONE EVENT, SEVERAL REGIMES

Most in-scope businesses already report incidents under other regimes. These have not been aligned, and a single event can trigger several obligations at once, to different recipients, on clocks that start at different moments.

REGIME	WHO REPORTS	WHAT IS REPORTED	DEADLINES
CRA	manufacturer of the product with digital elements	actively exploited vulnerability or severe incident affecting product security	24h early warning, 72h notification, 14 days or 1 month final report
NIS2 (as implemented nationally)	essential and important entities	significant incident	24h early warning, 72h notification
GDPR	controller	personal data breach	72h to the supervisory authority, and to data subjects without undue delay where the risk is high
DORA	financial entities	major ICT-related incident	4h initial notification from classification (max 24h from awareness), 72h intermediate report, 1 month final report

The Digital Omnibus package proposes a single entry point across these regimes, but it would consolidate the reporting channel rather than the obligations, and the proposals are still going through the legislative process.

CRA reporting obligations

What your business needs to know
before 11 September 2026

PENALTIES AND SUPERVISORY RISK

Breach of the reporting obligations sits in the CRA's highest penalty tier: fines of up to EUR 15 million or 2.5% of total worldwide annual turnover, whichever is higher, against EUR 10 million or 2% for other infringements.

Market surveillance powers may matter more than the fines. Authorities can require a product to be withdrawn from the market or prohibit it from being made available in the EU.

HOW CAN WE HELP?

1 Scoping and roles – we help our clients with assessing which of their products fall within the CRA, and in which role their business acts: manufacturer, importer or distributor.

2 Reporting readiness – we help our clients define what counts as a reportable event and put in place an internal process for deciding what to report, including how decisions not to report are documented. We advise on how CRA reporting aligns with NIS2, GDPR and DORA. We also help with establishing a single point of contact to facilitate communication between manufacturers and users.

3 Supply chain – we help our clients with reviewing supplier contracts to secure vulnerability information within the CRA deadlines, and the mirror commitments business customers expect from them.



4 CRA compliance exercise – we help our clients with product classification and conformity assessment routes, CE marking obligations, support periods and vulnerability handling, ahead of the CRA becoming fully applicable in December 2027.

CONTACT



SZYMON SIENIEWICZ
Counsel, Head of TMT/IP (Poland)
Tel +48 22 526 5042
Mob +48 665 052 724
szymon.sieniewicz@aglaw.com