

Cyber Resilience Act

Key requirements and deadlines for businesses



The CRA's first reporting requirements have applied since September 11, 2026.

The Cyber Resilience Act (CRA) sets mandatory cybersecurity requirements for products with digital elements throughout their lifecycle. Manufacturers must address security from development through vulnerability handling and updates.



Who is affected?

Product manufacturers

Primarily manufacturers of hardware and software with digital elements. Importers, distributors, and open-source stewards may also have obligations. Applicability must be assessed case by case.



What does it cover?

Security by design

Risk assessment, secure defaults, vulnerability management, security updates, technical documentation and, depending on the product, conformity assessment.



When?

Prepare now

The first reporting obligations already apply. Most remaining CRA requirements become fully applicable on December 11, 2027.

CRA timeline



Dec 10, 2024

CRA enters into force



Jun 11, 2026

Rules for conformity assessment bodies



Sep 11, 2026

Reporting obligations apply



Dec 11, 2027

CRA fully applicable

“ In short: Reporting obligations have applied since September 11, 2026. Organizational and technical preparations for full application should therefore already be underway.

Reporting obligations

24 h

Early warning

after becoming aware of an actively exploited vulnerability or a serious security incident

72 h

Main notification

with available information about the event and its impact

Then

Final report

14 days after a corrective measure becomes available or 1 month after the 72-hour notification

What companies should prepare now

Specific obligations depend on the company's role and product. However, affected manufacturers generally face the same organizational tasks:



Assess applicability and product portfolio

Which products fall within the scope – and what role does the company play under the CRA?



Assess cybersecurity risks

Systematically identify risks and include necessary safeguards in development and secure default settings.



Manage vulnerabilities and updates

Clearly define vulnerability handling, security updates and support periods across the product lifecycle.



Prepare documentation and conformity

Integrate technical documentation, evidence, conformity assessment and CE marking into processes in good time.

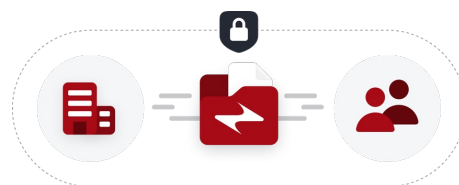


Establish reporting processes

Set responsibilities, escalation paths and reporting procedures to meet the CRA's short deadlines.

How netfiles supports you

CRA compliance is more than a documentation project. Development, vulnerability management, audits and collaboration with partners involve sensitive technical information that must be exchanged in a controlled manner.



Controlled data exchange

Securely share sensitive technical documents with internal and external participants.



Granular access permissions

Control precisely who can view, edit or download content.



Traceable activities

Activity logs support transparency and documented collaboration.



100% made & hosted in Germany

Company headquarters, development and hosting in Germany – for data protection, sovereignty and a clear legal framework.

Secure support for CRA requirements

Want to exchange sensitive technical documents and evidence securely with internal and external participants? Talk to us about your requirements.

[Get expert advice](#) →

+49 8677 91596-12



Made & hosted in Germany



ISO cert. · BSI C5 · SOC 2



GDPR-compliant

netfiles.com

Sources: European Commission – CRA Implementation, CRA Reporting, CRA Manufacturers (as of September 2026).

Note: This overview provides general information and does not constitute legal advice. Whether and to what extent a company or product is subject to the CRA must be assessed individually.