

Cyber Resilience Act

Die wichtigsten Pflichten und Fristen für Unternehmen



Seit 11. September 2026 gelten die ersten Meldepflichten des CRA.

Der Cyber Resilience Act (CRA) schafft verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen über ihren gesamten Lebenszyklus. Hersteller müssen Sicherheit von der Entwicklung bis zum Umgang mit Schwachstellen und Updates mitdenken.



Für wen?

Hersteller digitaler Produkte

Vor allem Hersteller von Hardware und Software mit digitalen Elementen. Auch Importeure, Händler und Open-Source-Stewards können Pflichten treffen. Die konkrete Betroffenheit ist individuell zu prüfen.



Worum geht es?

Security by Design

Risikobewertung, sichere Standardkonfiguration, Vulnerability Management, Sicherheitsupdates, technische Dokumentation und – je nach Produkt – Konformitätsbewertung.



Wann?

Jetzt vorbereiten

Die ersten Meldepflichten gelten bereits. Die übrigen wesentlichen CRA-Pflichten werden ab 11. Dezember 2027 vollständig anwendbar.

Die CRA-Timeline



10. Dezember 2024
CRA tritt in Kraft



11. Juni 2026
Regeln zu Konformitätsbewertungsstellen



11. September 2026
Meldepflichten gelten



11. Dezember 2027
CRA vollständig anwendbar

“ **Kurz gesagt:** Mit Stichtag 11. September 2026 laufen die Berichtspflichten. Die organisatorische sowie technische Vorbereitung auf die vollständige Anwendung sollte daher längst begonnen haben.

Meldepflichten

24 h

Frühwarnung

nach Bekanntwerden einer aktiv ausgenutzten Schwachstelle oder eines schwerwiegenden Sicherheitsvorfalls

72 h

Hauptmeldung

mit den verfügbaren Informationen zum Ereignis und seinen Auswirkungen

Danach

Abschlussbericht

14 Tage nach verfügbarer Korrekturmaßnahme bzw. 1 Monat nach der 72-Stunden-Meldung

Was Unternehmen jetzt vorbereiten sollten

Die konkreten Pflichten hängen von Rolle und Produkt ab. Für betroffene Hersteller führen die CRA-Anforderungen jedoch immer wieder zu denselben organisatorischen Aufgaben:



Betroffenheit und Produktportfolio prüfen

Welche Produkte fallen in den Anwendungsbereich – und welche Rolle hat das Unternehmen im CRA?



Cybersecurity-Risiken bewerten

Risiken systematisch erfassen und die notwendigen Schutzmaßnahmen bereits in Entwicklung und Standardkonfiguration berücksichtigen.



Schwachstellen und Updates organisieren

Vulnerability Handling, Sicherheitsupdates und Supportzeiträume über den Produktlebenszyklus fest definieren.



Dokumentation und Konformität vorbereiten

Technische Dokumentation, Nachweise, Konformitätsbewertung und CE-Kennzeichnung rechtzeitig in Prozesse integrieren.

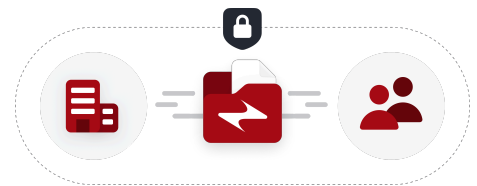


Reporting-Prozesse festlegen

Verantwortlichkeiten, Eskalationswege und Meldeprozesse so aufstellen, dass die kurzen CRA-Fristen eingehalten werden können.

Wie netfiles unterstützt

CRA-Compliance ist mehr als ein Dokumentationsprojekt. Bei Entwicklung, Vulnerability Management, Audits und der Zusammenarbeit mit Partnern entstehen sensible technische Informationen, die kontrolliert ausgetauscht werden müssen.



Kontrollierter Datenaustausch

Sensible technische Unterlagen sicher mit internen und externen Beteiligten teilen.



Granulare Zugriffsrechte

Präzise steuern, wer Inhalte sehen, bearbeiten oder herunterladen darf.



Nachvollziehbare Aktivitäten

Aktivitätenprotokolle unterstützen Transparenz und dokumentierbare Zusammenarbeit.



100 % made & hosted in Germany

Firmensitz, Entwicklung und Hosting in Deutschland – für Datenschutz, Souveränität und klare Rechtsräume.

CRA-Anforderungen sicher begleiten

Sie möchten sensible technische Unterlagen und Nachweise sicher mit internen und externen Beteiligten austauschen? Sprechen Sie mit uns über Ihre Anforderungen.

[Jetzt beraten lassen →](#)

+49 8677 91596-12



Made und hosted in Germany



ISO/BSI/SOC 2-zertifiziert



DSGVO-konform

netfiles.com

Quellen: Europäische Kommission – CRA Implementation, CRA Reporting, CRA Manufacturers (Stand: September 2026).

Hinweis: Dieser Überblick dient der allgemeinen Information und ersetzt keine rechtliche Beratung. Ob und in welchem Umfang ein Unternehmen oder Produkt dem CRA unterliegt, ist individuell zu prüfen.