

Anvendelsesområde

Hvad dækker Cyber Resilience Act?

Cyber Resilience Act (CRA) gælder for **produkter med digitale elementer**, der **gøres tilgængelige på markedet i EU** – uanset om de er produceret inden for eller uden for EU.

CRA omfatter hele **produktets livscyklus**: Fra design, udvikling og produktion, til support og opdateringer – og stiller krav til cybersikkerhed, risikohåndtering og ansvar ved sårbarheder.

Ifølge **artikel 2, stk. 1** gælder forordningen kun for produkter, hvis **tilsigtet formål eller rimeligt forudsigelige anvendelse** indebærer:

“en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.”

Det betyder, at produkter uden nogen form for kommunikationsforbindelse typisk **falder uden for CRA's anvendelsesområde** – mens netværkstilsluttede enheder, cloud-integrerede systemer og software med API-forbindelser i reglen er omfattet.

Definition: Et produkt med digitale elementer er ifølge artikel 3, stk. 1 i CRA:
“et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat”

Hvad er undtaget?

Visse produkter og sektorer er undtaget fra CRA, hvis de allerede er dækket af **eksisterende EU-lovgivning med tilsvarende eller strengere cybersikkerhedskrav**. Det gælder f.eks.:

- Medicinsk udstyr (MD/IVDR)
- Luftfarts- og bilindustrien
- Jernbanesystemer
- Maskiner omfattet af maskinforordningen
- Militært udstyr og produkter til national sikkerhed

Desuden er **tjenesteydelser** som SaaS, API'er og webapplikationer **ikke i sig selv omfattet**, da CRA kun gælder produkter – ikke ydelser.

Men: Hvis en tjeneste integreres i et fysisk eller softwareprodukt, skal producenten sikre, at det samlede produkt opfylder kravene, **herunder integrationer med eksterne komponenter**.

Open Source og mikrovirksomheder

- **Open source software (OSS)** er ikke undtaget pr. definition. Hvis en OSS-komponent bruges i et produkt, skal den leve op til kravene i CRA.
 - **OSS-forvaltere**, der udvikler og udgiver software **uden kommercielt formål**, er dog undtaget fra bøder og ansvar, jf. artikel 24 og præambel 120.
 - **Mikrovirksomheder** får lempelser på visse områder (fx vedr. sanktioner og rapporteringsfrister), men skal stadig overholde de væsentlige krav.
-

Hvad betyder "bragt i omsætning"?

Et produkt betragtes som "**bragt i omsætning**", når det **første gang gøres tilgængeligt på EU's marked** – enten ved salg, udlejning, gratis distribution eller på anden måde overdrages til en bruger uden for producentens organisation.

CRA gælder derfor ikke kun for produkter, der sælges, men også for f.eks. beta-versioner, open source-hardware eller gratis software, **så længe de stilles til rådighed for tredjepart**.

Eksempler:

- **En Android-app**, der distribueres via Google Play, betragtes som bragt i omsætning – den leveres som software til slutbrugeren og skal overholde CRA's krav som et produkt med digitale elementer.
 - **Et API**, der hostes og anvendes internt i en virksomhed, eller udelukkende stilles til rådighed som en tjeneste (f.eks. SaaS), **betrages som en tjenesteydelse**, og er **ikke omfattet** af CRA.
 - **En Android-app, der integrerer et eksternt API** (f.eks. til betaling, login eller cloud-funktioner), skal opfylde CRA-kravene, **hvor integrationen er væsentlig for appens funktionalitet**. Selvom API'et i sig selv er en tjenesteydelse, **skal app-producenten sikre, at API'et ikke underminerer cybersikkerheden** i det samlede produkt. Dette skal dokumenteres i den tekniske dokumentation, og være en del af cybersikkerhedsrisikovurderingen.
 - **Et smart home-device**, som f.eks. en internetforbundet termostat, der benytter en cloud-tjeneste til fjernstyring via en app, er også omfattet. Selvom cloudtjenesten i sig selv er en tjeneste, skal producenten dokumentere, at integrationen ikke underminerer sikkerheden – og at det samlede produkt opfylder CRA's krav.
-

Bemærk: Hvis en producent anvender tredjeparts-komponenter eller tjenester i et produkt med digitale elementer, skal de kunne dokumentere, at disse komponenter **ikke underminerer de væsentlige cybersikkerhedskrav** – uanset om leverandøren af disse komponenter selv er forpligtet af CRA.

Hvornår træder CRA i kraft?

CRA anvendes fra **11. december 2027**, med undtagelse af enkelte bestemmelser om indberetning, der gælder fra **11. september 2026**.

For detaljeret gennemgang af undtagelser, præcise definitioner og særlige tilfælde – se artiklerne 2–4 og præamblerne 53–58.

Last update: 2025-10-30 12:07:19