

Artikler

Hvad er artikler i CRA?

Artiklerne i EU-forordninger – herunder Cyber Resilience Act (CRA) – udgør den **juridisk bindende del** af retsakten.

Hvor præamblerne forklarer baggrund og hensigt, og bilagene indeholder tekniske krav og modeller, er det **artiklerne**, der definerer: - Hvem forordningen gælder for - Hvilke forpligtelser der gælder for producenter, importører og distributører - Hvad der udgør overensstemmelse - Sanktioner, overgangsbestemmelser og myndigheders rolle

Artiklerne er dermed **centrale for forståelse og efterlevelse** af CRA – men skal **læses i sammenhæng med præambler og bilag**.

Bemærk: Artiklerne beskriver **ikke tekniske detaljer** som dokumentationskrav, sårbarhedshåndtering, osv. Disse findes i bilagene og tilknyttede standarder.

Tematisk oversigt over artikler

Tema	Artikler	Beskrivelse
Generelt og anvendelsesområde	1–4	Formål, dækningsområde, definitioner og nationale undtagelser
Cybersikkerhedskrav og markedsadgang	6, 14	Hvornår må produkter bringes i omsætning, og hvilke krav skal være opfyldt
Produktklassificering	7–8, 12	Klassificering af vigtige og kritiske produkter og samspil med AI
Fabrikantens forpligtelser	13	Udvikling, risikovurdering, opdateringer, OSS, supportperiode
Andre aktørers roller	19, 20, 24	Importør, distributør og open source-forvaltere

Tema	Artikler	Beskrivelse
Overensstemmelse og dokumentation	27–32	Dokumentation, erklæringer og vurderingsprocedurer
Markedsovervågning og tilsyn	54–58, 91–94	Offentlige myndigheders rolle og indgriben
Sanktioner og ansvar	64, 121	Bødeniveau, aktørtyper og bødeansvar
Overgang og ikrafttræden	69, 126	Tidsfrister og overgangsregler

Udvalgte nøgleartikler

Herunder er centrale artikler, der ofte danner grundlag for compliance- og udviklingsarbejde:

- **Artikel 13 – Fabrikantens ansvar**
Definerer ansvar for cybersikkerhed i hele livscyklussen: design, risikovurdering, support og OSS.
- **Artikel 6 – Markedsadgang**
Et produkt må kun bringes i omsætning, hvis det overholder kravene i CRA.
- **Artikel 7 – Klassificering af vigtige produkter**
Produkter med digitale elementer, hvis primære funktion falder under en kategori i **Bilag III**, klassificeres som *vigtige produkter*.
De opdeles i **klasse I og II** afhængigt af cybersikkerhedsrisikoen, hvor **klasse II** kræver **strengere overensstemmelsesvurdering**.
Kommissionen kan ændre Bilag III via delegerede retsakter og skal senest 11. december 2025 fastsætte en teknisk beskrivelse af kategorierne.
- **Artikel 14 – Sårbarhedsovervågning og rapportering**
Producenter skal overvåge, håndtere og rapportere sårbarheder og hændelser – denne artikel træder i kraft allerede **11. september 2026**.
- **Artikel 27–28 – Formodet overensstemmelse og erklæring**
Produkter, der er i overensstemmelse med harmoniserede standarder, opnår formodning om overensstemmelse med kravene i denne forordning.
- **Artikel 31 – Teknisk dokumentation**
Dokumentationen skal være klar, fyldestgørende og ajourført – og skal være udarbejdet før produktet bringes i omsætning.

- **Artikel 91 – Overensstemmelsesorganer**
Fastlægger hvilke aktører der kan godkende produkter, og hvornår der kræves ekstern vurdering.

Hvad dækker artiklerne ikke?

Artiklerne udgør lovens rygrad – men **detaljerne findes andetsteds**:

Emne	Hvor du finder det
Tekniske cybersikkerhedskrav	Bilag I
Brugsvejledninger og metadata	Bilag II
SBOM-krav og supportperiode	Bilag I og VII
Dokumentationsstruktur	Bilag VII
Overensstemmelsesprocedurer	Bilag VIII
Fortolkningshjælp	Præamblerne

Du bør derfor **læse artiklerne sammen med præambler og bilag** – samt relevante standarder (f.eks. EN 303 645) – for at få det fulde billede.

Relaterede sektioner

- [06_bilag.md](#) – Bilagenes funktion og krav
- [04_præambler.md](#) – Juridisk fortolkning og hensigter
- [07_klassificering_af_produkter.md](#) – Produktklasser og deres konsekvenser

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