

Præambler

Hvad er præambler i CRA (og EU-forordninger generelt)?

Præamblerne er den indledende del af en EU-retsakt og tjener til at forklare **formål, hensigt og fortolkningsramme** for reglerne. De er **ikke juridisk bindende**, men har **betydning for fortolkningen** af de bindende artikler og bilag.

I CRA anvendes præamblerne til at: - forklare formålet med specifikke krav, - præcisere forventninger til fabrikanter, - guide myndigheder og domstole i fortolkning af reglerne.

Selvom de typisk anvender formuleringer som "*bør*", "*kan*" og "*hensigten er*", anvendes de i praksis aktivt af: - markedsovervågningsmyndigheder, - domstole i fortolkningssager, - udviklingsteams og compliance-ansvarlige.

Derfor er præamblerne væsentlige at kende og inddrage – også selvom kun artikler og bilag er juridisk bindende.

Udvalgte præambler, grupperet efter tema

Herunder er centrale præambler opdelt i tematiske grupper, med forklarende noter. Det skal dog understreges, at præamblerne **bør læses direkte i forordninge**

▮ Væsentlige cybersikkerhedskrav

Præambel	Emne	Beskrivelse
22	SBOM	SBOM skal kunne leveres til markedsovervågningsmyndigheden på anmodning.
38	Kendte sårbarheder	Et produkt må ikke bringes i omsætning, hvis der findes kendte sårbarheder.
54	Cybersikkerhedsrisikovurdering	Producenter skal foretage en risikovurdering, der dækker både cybersikkerhed og produktegenskaber.

Præambel	Emne	Beskrivelse
55	Undtagelser fra krav	Fravigelser fra væsentlige krav skal være dokumenterede og teknisk begrundede.
64	Secure by default	Produkter, der bringes i omsætning, skal være sikre som udgangspunkt.
65	Indberetning til ENISA og CSIRT	Fabrikanter skal indberette aktivt udnyttede sårbarheder til relevante myndigheder.
67	Underretning af brugere	Brugere bør informeres om hændelser og korigerende handlinger.
77	SBOM og 3. parts komponenter	Krav om håndtering af sårbarheder i tredjepartssoftware – også uden offentliggørelse af SBOM.

□ Produktets livscyklus og ansvar

Præambel	Emne	Beskrivelse
34	3. parts komponenter	Producenten bør sikre, at alle integrerede tredjepartskomponenter – herunder OSS – opfylder cybersikkerhedskravene.
35	Komponenter før CRA	Hvis en komponent er integreret før CRA trådte i kraft, bør producenten stadig vurdere overholdelse.
36	Ufærdig software (beta)	Software i beta må bringes i omsætning midlertidigt, uden fuldt CRA-krav.
39	Væsentlige ændringer	Ændres produktets tilsigtede formål, kræves ny vurdering og overholdelse.

Præambel	Emne	Beskrivelse
59	Supportperiode	Supportperioden bør fastsættes i forhold til forventet brugstid.
60	Min. supportperiode	Som udgangspunkt bør supporten vare mindst 5 år – medmindre brugstiden er kortere.
61	Ved ophør	Ved ophør af support bør kildekoden offentliggøres eller overdrages.

□ Klassificering og overensstemmelse

Præambel	Emne	Beskrivelse
43	Vigtige produkter	Definition af vigtige produkter (Bilag III).
44	Klasse I og II	Klasse II har højere cybersikkerhedsrisiko og strengere krav.
45	Krav til Klasse II	Krav om tredjepartsvurdering for produkter i Klasse II.
81	Overensstemmelseserklæring	Producenter skal afgive en erklæring om overensstemmelse med cybersikkerhedskrav.
89	CE-mærkning	CE-mærket dokumenterer overensstemmelse med CRA.
90	Overensstemmelsesprocedurer	Definerer hvilken overensstemmelsesprocedure der anvendes.
91	Ansvarlig instans	Viser, hvem der kontrollerer krav – afhænger af klassificering.

□ OSS og mikrovirksomheder

Præambel	Emne	Beskrivelse
120	Sanktioner og undtagelser	Mikrovirksomheder og OSS-forvaltere er fritaget fra visse bøder, fx for forsinket indberetning.

□ Indberetning og markedsovervågning

Præambel	Emne	Beskrivelse
63	Kontaktpunkt	Fabrikanten bør have et centralt kontaktpunkt for sårbarhedsrapportering.
70–74	Indberetning og myndigheder	Fastlægger rammer for myndighedsindberetning.
107	Markedsovervågning	Medlemsstater skal udpege markedsovervågningsmyndigheder.
121	Bøder til enkeltpersoner	Medlemslande kan tillade bøder til fysiske personer – afhænger af national lovgivning.
126	Ikrafttrædelse	CRA træder i kraft 11. december 2027, visse rapporteringskrav dog fra 11. september 2026.

Sammenfatning

Præamblerne i CRA giver et unikt indblik i **intentionerne bag lovteksten**. De understreger, at ansvar følger hele produktets livscyklus, og at cybersikkerhed også omfatter integrationer med fx OSS eller API'er – også når disse ikke er direkte omfattet af CRA.

CRA's tilgang til fortolkning og markedsovervågning er risikobaseret og helhedsorienteret – og præamblerne spiller en væsentlig rolle i, hvordan den forstås og håndhæves i praksis.

Vigtigt: Brug præamblerne aktivt i dokumentation, risikovurdering og compliance-arbejde – særligt når kravene i artiklerne kræver fortolkning eller uddybning.

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