

Markedsovervågning og bøder

Cyber Resilience Act (CRA) forudsætter, at der føres effektivt tilsyn med markedet for produkter med digitale elementer. Dette sker gennem nationale markedsovervågningsmyndigheder i hvert EU-land, som har ansvar for at kontrollere overholdelsen af CRA og udstede sanktioner ved overtrædelser.

Nationale markedsovervågningsmyndigheder

Hver medlemsstat skal udpege én eller flere kompetente myndigheder til at føre tilsyn med CRA (jf. artikel 107). Disse myndigheder har bl.a. beføjelse til at:

- **Efterspørge teknisk dokumentation** og SBOM ved stikprøvekontrol
- **Påbyde tilbagekaldelser eller stop for markedsføring**, hvis produktet ikke opfylder CRA
- **Vurdere supportperioder** og anmode om forlængelse, hvis den anses for for kort
- **Koordinere med andre medlemsstater**, hvis produktet markedsføres i hele EU

Myndighederne vurderer ikke kun teknisk dokumentation, men kan også inddrage **geopolitiske og politiske hensyn** (jf. præambel 54).

Sanktioner og bøder

CRA indeholder rammer for **administrative sanktioner** ved overtrædelser – dog med plads til nationale tilpasninger. Bøder kan pålægges følgende aktører:

- **Fabrikanter**
- **Importører og distributører**
- **Tjenesteudbydere**
- **(I visse tilfælde) enkeltpersoner** – hvis national ret tillader det (præambel 121)

Niveau for bøder

Overtrædelse	Bøde

Overtrædelse	Bøde
Overtrædelse af væsentlige cybersikkerhedskrav eller fabrikantansvar	Op til 15 mio. EUR eller 2,5 % af global årsomsætning
Brud på teknisk dokumentation, importør/distributørpligter	Op til 10 mio. EUR eller 2 % af global årsomsætning
Urigtige eller mangelfulde oplysninger til myndigheder	Op til 5 mio. EUR eller 1 % af global årsomsætning

▮ **Bemærk:** Medlemsstater fastsætter selv præcise bødeniveauer. CRA kræver blot, at sanktioner er **effektive, afskrækkende og proportionelle**.

Undtagelser og lempelser

- **Mikrovirksomheder** får lempelse ift. **tidsfrister** for rapportering og **kan fritages for bøder** i visse tilfælde (præambel 120)
- **Open source-forvaltere** er undtaget fra bøder, **hvis softwaren er gratis og ikke kommerciel** (jf. artikel 24 og præambel 120)
- **Enkeltpersoner** kan kun pålægges bøder, hvis medlemsstatens nationale lovgivning tillader det – og da skal der tages hensyn til deres **økonomiske forhold og levevilkår**

Markedstilsyn i praksis

Markedsovervågningsmyndigheder vil i praksis fokusere på:

- **Stikprøver og risikobaseret kontrol** af CE-mærkede produkter
- Overvågning af **supportperioder** og opdateringspraksis
- Vurdering af, om produktet er **“Secure by Default”**
- Undersøgelser ved **hændelser eller kendte sårbarheder**

▮ Produkter, der udgør en væsentlig cybersikkerhedsrisiko, **kan kræves trukket tilbage fra hele EU-markedet**, selv hvis de teknisk overholder CRA (jf. præambel 57 og artikel 54).

Myndighedernes ansvar og samarbejde

CRA lægger vægt på **EU-dækkende koordinering**, herunder:

- Samarbejde gennem **ENISA**
- Sammenlignelige sanktioner mellem medlemslande
- Offentliggørelse af **supportstatistikker** (præambel 32)
- Fælles retningslinjer for risikoevaluering og fortolkning

▮ CRA's markedstilsynsmodel bygger på både **teknisk dokumentation, risikovurdering og organisatorisk ansvar** – og adskiller sig derved fra klassisk produktkontrol.

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