

Forkortelser og definitioner

Denne sektion samler de vigtigste forkortelser og centrale definitioner, som benyttes i dokumentationen vedrørende Cyber Resilience Act (CRA). Den er tænkt som et opslagsværk, der kan konsulteres på tværs af sektionerne.

Forkortelser

Forkortelse	Betydning
CRA	Cyber Resilience Act – Forordning (EU) 2024/2847 om cybersikkerhedskrav for produkter med digitale elementer
OSS	Open Source Software – software med offentlig tilgængelig kildekode, som typisk distribueres gratis
SBOM	Software Bill of Materials – en liste over alle komponenter (inkl. open source) i et softwareprodukt
CE-mærkning	EU's mærkningsordning for produkter, som opfylder relevante krav i EU-lovgivning
ENISA	European Union Agency for Cybersecurity – EU's cybersikkerhedsagentur
CSIRT	Computer Security Incident Response Team – en enhed der håndterer cybersikkerhedshændelser, fx ved aktiv udnyttelse
ADCO	Administrative Cooperation Group – netværk mellem medlemsstaternes markedsovervågningsmyndigheder
API	Application Programming Interface – grænseflade til kommunikation mellem forskellige softwarekomponenter
Modul A	Intern kontrol – overensstemmelsesvurdering uden involvering af tredjepart
Modul B	EU-typeafprøvning – vurdering af produktdesign og cybersikkerhed hos et bemyndiget organ

Forkortelse	Betydning
Modul C	Overensstemmelse med typegodkendelse – fabrikanten sikrer overensstemmelse i produktionen
Modul H	Fuld kvalitetssikring – omfattende vurdering af kvalitetsstyringssystem med løbende kontrol

Centrale definitioner (jf. artikel 3)

Produkt med digitale elementer

et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat.

Fabrikant

En fysisk eller juridisk person, som fremstiller eller får fremstillet et produkt og markedsfører det under eget navn eller varemærke.

Bringe i omsætning

Den første tilgængeliggørelse af et produkt på EU-markedet, uanset om det sælges, gives gratis eller udlejes.

Gøre tilgængelig på markedet

Enhver levering af et produkt med digitale elementer til distribution, forbrug eller anvendelse på EU-markedet.

Supportperiode

Den tidsperiode, i hvilken en fabrikant forpligter sig vedligeholde produktets overensstemmelse med de væsentlige cybersikkerhedskrav i hele den angivne supportperiode gennem bl.a. opdateringer og sårbarhedshåndtering.

Sårbarhedshåndtering

De processer og mekanismer, som fabrikanten har etableret for at identificere, afhjælpe og kommunikere om sikkerhedssårbarheder.

Koordineret offentliggørelse af sårbarheder

En politik og praksis, hvor en fabrikant samarbejder med eksterne parter (fx sikkerhedsforskere) om ansvarlig deling og udbedring af sårbarheder.

Væsentlig ændring

Enhver ændring i et produkts design eller anvendelse, der kan påvirke produktets overensstemmelse med cybersikkerhedskravene, herunder ændringer i formål, komponenter eller netværkstilslutning.

Harmoniseret standard

En teknisk specifikation, udarbejdet af en europæisk standardiseringsorganisation og offentliggjort i EU-Tidende, der understøtter overholdelse af lovgivning.

NANDO

New Approach Notified and Designated Organisations – EU's officielle database over bemyndigede organer, der er udpeget af medlemsstaterne til at udføre overensstemmelsesvurderinger i henhold til harmoniseret lovgivning, herunder CRA. Organerne vurderer f.eks. om kritiske produkter opfylder kravene i forordningen, når proceduren kræver tredjepartsinvolvering (fx Modul B eller H).

Bemærk: Definitionerne er forenklede og tilpasset læsbarhed. Ved tvivl bør den præcise ordlyd i artikel 3 konsulteres.

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