Zoé Elkær Nicot
Ministeriet for Samfundssikkerhed og Beredskab
Slotsholmsgade 12
1216 København K

03-02-2026
EMN-2026-00152
1833966
Andreas Barfod Suhr

Danske Regioners høringssvar: Europa-Kommissionens forslag til revision af Cyber Security Act

Ministeriet for Samfundssikkerhed og Beredskab har den 20. januar 2026 anmodet Danske Regioner om bemærkninger til forslag til Europa-Kommissionens forslag til revision af Cyber Security Act. Danske Regioner kvitterer for muligheden for at afgive høringssvar og fremsender høringssvar på vegne af de fem regioner.

Det er Danske Regioners opfattelse, at ændringerne primært vil have praktisk betydning for EU-institutionerne, særligt ENISA, og sekundært de kompetente, nationale myndigheder. Det forventes ydermere, at revisionen potentielt kan have positiv indvirkning på leverandørsamarbejde, og at leverandørstyringen vil kunne lettes, hvis der opnås de forventede gevinster vedr. certificeringen af leverandører.

Danske Regioner ser frem til, at det på baggrund af revisionsforslaget bliver muligt at indhente mere standardiseret vejledning samt oplysninger om trusler og sårbarhedshåndtering fra EU's cybersikkerhedsinstitutioner, og ønsker, at MSSB løbende holder Danske Regioner orienteret om nyt ift. revisionsforslaget.

Konkrete bemærkninger

Udover de overordnede overvejelser, har Danske Regioner en række tekstnære kommentarer og forslag til yderligere præcisering at høringsmaterialet, som præsenteres i det følgende.

Operationalisering af proportionalitet

Forslaget lægger flere steder vægt på en risikobaseret og proportional tilgang til cybersikkerhed, herunder i relation til både certificering og ICT-forsyningskædesikkerhed. Danske Regioner finder det positivt, at proportionalitet eksplicit fremhæves, men bemærker samtidig, at forslaget i

DANSKE REGIONER
DAMPFÆRGEVEJ 22
2100 KØBENHAVN Ø
+45 35 29 81 00
REGIONER@REGIONER.DK
REGIONER.DK

begrænset omfang præciserer, hvordan proportionalitet konkret skal operationaliseres for organisationer, der varierer betydeligt i størrelse, kompleksitet og modenhed. Danske Regioner anbefaler derfor, at der i det videre arbejde overvejes:

- en tydeligere kobling mellem krav og organisatorisk kontekst (fx størrelse, organisationstype og sektor),
- samt supplerende vejledning eller rammer, der understøtter ensartet anvendelse på tværs af medlemsstater.

Præcisering af "cyber posture of entities"

Der introduceres muligheden for certificering af "cyber posture of entities" som et nyt element i det europæiske cybersikkerheds-certificeringsframework. Danske Regioner bemærker, at:

- begrebet ikke er nærmere defineret i forslaget,
- og at forholdet til eksisterende rammer og krav (f.eks. NIS2) ikke er klart beskrevet.

Danske Regioner anbefaler derfor, at der arbejdes videre med:

- en klarere begrebsmæssig afgrænsning af "cyber posture",
- en tydelig beskrivelse af, hvilke elementer en sådan posture forventes at omfatte,
- samt hvordan overlap og dobbeltregulering i forhold til eksisterende compliance-forpligtelser kan undgås.

Fælles framework for ICT-forsyningskæder

Danske Regioner støtter ambitionen om at styrke sikkerheden i ICT-forsyningskæder gennem et fælles EU-framework, herunder fokus på ikke-tekniske risikofaktorer og afhængigheder. Samtidig anses det som væsentligt, at der tages højde for praktiske og kontraktuelle realiteter, særligt for offentlige og kritiske aktører, herunder:

- langvarige kontraktforpligtelser,
- anvendelse af fællesoffentlige eller nationale rammeaftaler,
- samt begrænset mulighed for hurtigt leverandørskifte.

Danske Regioner anbefaler derfor, at der ifm. implementeringen sikres:

- klare overgangsbestemmelser,
- realistiske tidsrammer,
- og tydelig vejledning om håndtering af eksisterende kontraktforhold.

National kompetence og grænseflader

Forslaget styrker ENISA's rolle markant, herunder med mere operationelle opgaver, samtidig med at det fastslås, at nationale CSIRT's og myndigheder fortsat har deres ansvar. Danske Regioner finder det positivt, at national

kompetence respekteres, men anbefaler, at der i den videre udmøntning lægges vægt på:

- klare grænseflader mellem ENISA's understøttende rolle og nationale myndigheders ansvar,
- samt tydelig kommunikation om roller og ansvar i praksis.

Fælles principper og referencerammer

Forslaget lægger vægt på harmonisering og en risikobaseret tilgang. Danske Regioner anbefaler, at begrebet "risikobaseret" i højere grad operationaliseres, f.eks. gennem fælles principper eller referencerammer, der kan understøtte ensartet anvendelse på tværs af medlemsstater og sektorer. Dette vil styrke harmonisering på tværs af medlemsstaterne og dets enheder og bedre praktisk implementering.

Behov for baseline-krav og metoder

For mindre og mellemstore organisationer kan det være en væsentlig fordel, hvis der udvikles fælles europæiske baseline-krav og metoder, som kan anvendes som et minimumsudgangspunkt. Dette vil kunne understøtte proportionalitet, reducere kompleksitet og fremme ensartet praksis uden at forhindre risikobaserede tilpasninger.

Hændelsesrapportering

Forslaget om et fælles single entry point for hændelsesrapportering er positivt. I den forbindelse anbefales det at afklare:

- hvilket rapporteringssprog der forventes anvendt,
- samt hvordan nationale myndigheder og sektorspecifikke tilsyn kan integreres teknisk i løsningen, således at organisationer reelt kan rapportere én gang til ét sted og opfylde flere forpligtelser samtidigt.

Præcisering af vejledninger og anbefalinger

I takt med at ENISA's rolle styrkes, anbefales det, at der skabes klarhed og gennemsigtighed omkring ENISA's vejledninger og anbefalinger, herunder:

- hvilke vejledninger der aktuelt anses som gældende reference,
- og hvilke der er udfaset eller erstattet.

Dette vil understøtte ensartet anvendelse og reducere usikkerhed hos omfattede enheder.

Fælles metoder for konsekvensanalyser

Forslaget lægger op til, at der gennemføres økonomiske konsekvensanalyser forud for fastlæggelse af foranstaltninger vedrørende ICT-forsyningskæder. Danske Regioner anerkender behovet for et oplyst beslutningsgrundlag, men er samtidig bekymrede for, at sådanne analyser, hvis de ikke i videst muligt

omfang baseres på fælleseuropæiske metoder, kan medføre et øget ressourceforbrug for omfattede enheder. Det anbefales derfor, at analyserne i videst muligt omfang standardiseres, koordineres og stilles til rådighed centralt for at undgå parallelle og overlappende vurderinger.

Frihed i valg af framework

I relation til European Cybersecurity Skills Framework (ECSF) anbefales det, at enheders dokumenterede arbejde efter ECSF anerkendes som et positivt bidrag til compliance, samtidig med at alternative frameworks fortsat kan anvendes – forudsat at roller, ansvar, opgaver og kompetencer er klart defineret og dokumenteret.

Fælles baseline for informationsklassifikation

For kritiske sektorer omfattet af NIS2 kan det overvejes, om en fælles europæisk baseline for informationsklassifikation, eller krav om dokumenteret klassifikationsskema mappet mod EUCI, kan understøtte ensartet håndtering af følsomme oplysninger på tværs af grænser, sektorer og enheder.

Økonomiske konsekvenser

Danske Regioner forventer, at der vil være økonomiske konsekvenser som følge af ændringerne i forordningen. Sagen ønskes derfor medtaget på Lov- og Cirkulæreprogrammet med henblik på forhandling af lovforslagets konsekvenser for regionernes økonomi, jfr. Det Udvidede Totalbalanceprincip (DUT) i henhold til VEJL nr. 63 af 09/10/2007.

Venlig hilsen

Danske Regioner

v/ Andreas Barfod Suhr, Seniorkonsulent