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

19-02-2026
EMN-2026-00152
1838494
Andreas Barfod Suhr

Danske Regioners supplerende 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 Europa-Kommissionens forslag til revision af Cyber Security Act, og Danske Regioner afgav 4. februar sit høringssvar på vegne af regionerne. 6. februar udsendte ministeriet supplerende høringsmateriale og en præcisering af, at høringen af 20. januar vedrørte forslaget til forordningen, og den nye høring vedrørte forslaget til direktivet. Danske Regioner fremsender hermed supplerende høringssvar på vegne af regionerne, og anmoder om at høringssvaret vedr. direktivet ses i sammenhæng med høringssvaret afgivet 4. februar 2026 vedr. forordningen.

Danske Regioner ser overordnet positivt på de foreslåede ændring af direktivet, og ser frem til at se den konkrete udmøntning i en revision af den danske NIS2-lov. Udover kommentarerne i nærværende høringssvar, har Danske Regioner en forventning om, at Sundhedsdatastyrelsen i regi af DCISSund, repræsenterer alle aktørerne i sundhedsvæsenet – herunder også regionerne, hvilket forventes afspejlet i deres involvering i arbejdet.

Af ændringerne i NIS2-direktivet, er de mest relevante for regionerne at det bliver muligt for medlemslandene at stille krav om en certificering (udviklet af ENISA indenfor ECCF – European Cybersecurity Certification Framework) som bekræftelse på NIS2 efterlevelse (compliance) for enheder underlagt NIS2. Der ønskes dog visse præciseringer omkring certificering. Derudover ser Danske Regioner det som et opmærksomhedspunkt, at medlemslandene skal indarbejde post-quantum cryptography (PQC) i deres nationale cyber security-strategier. Tiltaget vurderes som værende fornuftigt, men kan medføre store implementeringsudgifter for regionerne. Endeligt bifalder Danske Regioner kravet om at medlemslandene skal sikre, at der ved ransomware-angreb deles informationer om angrebene, herunder om der er betalt løsesum. Der ses dog et stort behov for sikker deling af disse informationer, hvilket kræver teknisk og governance-mæssig understøttelse.

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

Det ønskes, at MSSB løbende holder Danske Regioner orienteret om nyt ift. revisionsforslagene samt implementering i dansk lovgivning.

Konkrete bemærkninger

Som supplement til de allerede afgivne input vedrørende forslaget til revision af NIS2-Direktivet, har Danske Regioner en række konkrete bemærkninger og opmærksomhedspunkter for regionernes område:

<u>Certificering og tilsyn</u>

- 'Union Cyber posture' bruges som et generelt referencepunkt for EU's standpunkt på cyber-området (s. 1-2), og ift. certificeringsmekanismen som et muligt certificeringsgrundlag (s. 2, 3, 8, 13), mens samme begreb bruges vedr. certificering specifikt for at demonstrere compliance med Art. 21 (s. 13). Begrebet ønskes defineret ift. certificeringen, altså om der er tale om certificering i efterlevelse af Art. 21, eller i en bredere forstand.
- Det formodes, at det, at enheder underlagt NIS2 vil kunne opnå certificering, vil gælde for regionerne (pba. s. 5). Det er uklart, hvad denne certificering vil kunne erstatte, andet end 'compliance-forpligtelser', og spørgsmålet er, om det kan erstatte tilsyn, og hvis ikke, hvilke 'compliance-forpligtelser' der så henvises til.
- Jf. s. 13, (9) stk. 5 beskrives, at når en enhed opnår certificering og derved demonstrerer compliance, må den kompetente myndighed ikke stille yderligere krav til tilsyn (Art. 32 (2), stk. b og Art. 33 (2), stk. b). Igen er det uklart, hvad certificeringen kan erstatte, idet det kan udledes som om der fortsat skal føres tilsyn, trods certificering. I så fald er det uklart, hvori lettelsen består.
- Certificering synes umiddelbart at være positivt og kan sikre en ensartet tilgang til sikringen af kravet om forsyningskædesikkerhed. Der vil formodentlig stadigvæk være en usikkerhed omkring, hvordan kravet i NIS2 om forsyningskædesikkerhed efterleves overfor leverandører, der ikke selv er omfattet af NIS2 kravene direkte (og dermed ikke umiddelbart er i scope for certificeringsordningen). Afhængigt af den konkrete implementering kan der potentielt være nye udgifter forbundet hermed, men det må afvente en mere konkret udmøntning af direktivet i dansk lov og mere konkret viden om den certificeringsordning, der tilbydes.

<u>Indmelding af ransomware-angreb</u>

- Bestemmelser vedr. indmelding af ransomware-angreb til den lokale CSIRT/relevante myndigheder er et fornuftigt krav, og vil øge viden om karakteren af denne særlige form for kriminalitet, og give myndigheder bedre muligheder for at få overblik over problemets størrelse. Det forventes, at regionerne vil skulle indmelde disse. Det ønskes dog

tydeliggjort, om bestemmelsen også gælder forsøg på ransomware-angreb, som det er lykkes regionerne af modstå.

- Danske Regioner ser meget gerne et styrket samarbejde på tværs af lande, i forhold til at kunne beskytte borgernes sundhedsdata og regionernes systemer. Med øget samarbejde og udveksling af sensitive informationer om f.eks. sårbarheder og hændelser opstår imidlertid også et behov for at værne om fortroligheden, f.eks. ved at skabe de nødvendige rammer for fortrolighed samt sikre systemer, som kan understøtte delingen. Denne del vurderer Danske Regioner med fordel kunne italesættes tydeligere som en væsentlig forudsætningsskabende præmis.
- I forlængelse af ovenstående ønskes det tydeliggjort, om ENISA's 'Cross-border cybersecurity risk assessment report' vil blive gjort tilgængelig for regionerne.

<u>Øvrige bemærkninger</u>

- På s. 7 under (3) nævnes, at scope-relaterede bestemmelser vedr. bl.a. healthcare providers bør klarlægges for at sikre juridisk entydighed og reducere compliance-byrder, uden at denne type bestemmelser nævnes andre steder i dokumentet, ud over en reference til "European action plan on the cybersecurity of hospitals and healthcare providers" som en del af de øvrige EU-initiativer (s. 2). Det ønskes tydeliggjort, om det er dette initiativ, der menes at kunne klarlægge ovenstående byrder og bestemmelser.
- Danske Regioner vurderer at kravet om post-quantum cryptography (PQC) er relevant, udviklingen af kvantecomputere taget i betragtning. Det skal dog bemærkes, at en overgang til PQC potentielt er en meget omkostningstung øvelse for regionerne. Sundhedssektoren er i den forbindelse særligt sårbar, idet sundhedsdata har en karakter, hvor brud på fortroligheden kan være kritisk i mange år fremadrettet (+100år) til forskel for andre informationer, hvor f.eks. den teknologiske udvikling kan gøre brud på fortrolighed mindre kritisk over tid. I forhold til PQC betyder det, at sundhedssektoren er særlig udsat.

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