ERHVERVSMINISTERIET

Høringsnotat vedrørende udkast til lovforslag om cybersikkerheds-certificering (Lov om cybersikkerhedscertificering)

Lovforslaget gennemfører forordningen om cybersikkerhed, der bl.a. skal etablere en fælles ramme for certificering af cybersikkerhed i EU. Forordningen træder endeligt i kraft 28. juni 2021.

Med lovforslaget udpeges Sikkerhedsstyrelsen som myndighed for cybersikkerhedscertificering i Danmark, og der fastsættes regler for, hvordan styrelsen fører kontrol med de forskellige aktører på området.

Lovforslaget skal dermed bidrage til at sikre, at danske virksomheder frivilligt kan få certificeret produkter, tjenester eller processer inden for informations- og kommunikationsteknologi. Certificeringen dokumenterer, at sikkerheden i et produkt, en tjeneste eller proces er på et vist niveau, typisk ved at produktet er produceret i overensstemmelse med en eller flere standarder. Med lovforslaget sikres det ydermere, at certificeringen sker under regulerede forhold, som Sikkerhedsstyrelsen overvåger.

Lovforslaget er sendt i offentlig høring fra 19. oktober til 16. november 2020. Lovforslaget fremgår af regeringens lovprogram med planlagt fremsættelse januar II 2021.

Der er i alt modtaget høringssvar fra fem af i alt 33 eksterne høringsparter, som er hørt undervejs. Heraf har tre haft bemærkninger til udkastet til lovforslag.

De væsentligste bemærkninger fra de hørte parter til de enkelte emner i lovudkastet gennemgås og kommenteres nedenfor.

Derudover har visse høringssvar givet anledning til enkelte redaktionelle ændringer og præciseringer i lovteksten og bemærkningerne. Disse ændrer ikke ved substansen i det pågældende forslag og omtales derfor ikke nærmere i dette notat.

2. Generelle bemærkninger

Lovforslaget er overordnet set blevet positivt modtaget. Der er generelt opbakning til at indføre certificeringsordninger inden for cybersikkerhed i produkter, tjenester og processer.

Dansk Industri (DI) udtrykker generelt tilslutning til lovforslaget og de kommende certificeringsordninger og udtrykker især tilfredshed med, at det er en fælleseuropæisk ordning, så virksomhederne ikke skal leve op til forskellige regler og krav i forskellige lande. Derudover udtrykker DI et ønske om, at det undersøges, om der kan være synergi ved at koordinere de nye europæiske cybersikkerhedscertificeringsordninger med en mærkningsordning for it-sikkerhed og dataanvendelse, som DI og en række danske partnere i øjeblikket arbejder på. DI gør opmærksom på, at der er både

ligheder og væsentlige forskelle på de opgaver, Sikkerhedsstyrelsen varetager i dag med bemyndigelse af overensstemmelsesvurderingsorganer inden for bestemte områder, og så cybersikkerhed, hvorfor det er nødvendigt med faglige kompetencer.

Dansk Erhverv & Teleindustrien (DE & TI) udtrykker generel opbakning til lovforslaget og hensigten med at øge sikkerheden i IKT-produkter, -processer og -tjenester. DE & TI påpeger dog, at der kan gå lang tid, før der kommer europæiske certificeringsordninger på grund af den måde, som ordninger bliver vedtaget på i EU-regi. Herudover påpeges en mulig udfordring i, at de konkrete certificeringsprodukter bliver så omkostningstunge, at det i praksis kan favorisere større virksomheder – og dermed virke konkurrenceforvridende f.eks. inden for markedet for bredbåndsløsninger.

Forbrugerrådet TÆNK (TÆNK) er generelt positive over for lovforslaget og påpeger, at certificeringsordninger kan medvirke til at øge trygheden og fremme tilliden til digitaliseringen, samt til at styrke forbrugernes databeskyttelse. Det er et område, som ligger TÆNK meget på sinde bl.a. fordi IoT-produkter (forbrugerprodukter der kan tilsluttes internettet), ifølge TÆNK, ofte er kendetegnet ved en kombination af utilstrækkelig sikkerhed og problematisk indsamling af data, der deles med tredjepart.

Bemærkninger til konkrete emner:

Kommenteringen af høringssvarene vil ske med udgangspunkt i følgende overordnede opdeling:

3.1. Kompetencer og finansiering
3.2. Frivillighed i certificeringsordningerne
3.3. Sammenhæng med øvrige mærkningsordninger
3.4. Adgang til virksomhederne
3.5. Information til brugerne
3.6. Ensartede definitioner

3.1 Kompetencer og finansiering

Dansk Industri (DI) bemærker, at det er væsentligt, at Sikkerhedsstyrelsen trækker på kompetencer fra blandt andet Center for Cybersikkerhed og parterne bag DI's mærkningsordning for cybersikkerhed og dataansvarlighed.

Dansk Erhverv & Teleindustrien (DE & TI) anfører, at det er vigtigt, at SIK får de nødvendige kompetencer og ressourcer tilført, da opgaven vil kræve begge dele. DE & TI vurderer, at det afsatte beløb på 2,7 mio. kr. til at varetage myndighedsopgaven kan virke utilstrækkeligt henset til, at SIK skal kunne behandle klager, foretage kontroller m.v., der også kræver øgede kompetencer.

Kommentar
Ved indplaceringen af opgaven om certificering af cybersikkerhed er der lagt vægt på, at den valgte myndighed har kompetencer og erfaring med tilsvarende myndighedsudøvelse. I hovedtræk vil det sige arbejdet med at påse overensstemmelse med relevante standarder og etablering, kvalitetssikring og kontrol af et certificeringssetup, der indeholder både akkreditering og bemyndigelse af overensstemmelsesvurderingsorganer mv. Det har Sikkerhedsstyrelsens omfattende erfaring med fra blandt andet fyrværkeri-, gas-, og metrologiområdet.

Det anerkendes, at der ved løsning af den ny opgave skal ske opbygning af både kompetencer og kapacitet. Undervejs i det arbejde trækker SIK på blandt andre Center for Cybersikkerhed (CFCS) og Erhvervsstyrelsen (ERST), som kan yde relevant faglig sparring. CFCS kommer til at få en rådgivende funktion som faglig sparringspartner, men vil ikke bistå SIK i forbindelse med tilsyn og kontrolarbejde hos virksomheder.

Cybersikkerhed er et område i hastig vækst, og det vil formentlig afspejle sig i antallet af certificeringer i de kommende år. Udviklingen er dog behæftet med usikkerhed, blandt andet fordi arbejdet med certificeringsordningerne er blevet forsinket som følge af COVID-19. For at håndtere den udfordring, er der lagt op til en genforhandling af områdets finansiering i 2023.

3.2 Frivillighed i ordningerne

Dansk Erhverv & Teleindustrien (DE og TI) skriver, at det er positivt, at certificeringsordningerne er frivillige og gør derudover opmærksom på, at det bør fremgå tydeligt, hvis nogle kategorier af produkter, tjenester eller processer bliver omfattet af obligatorisk certificering (fx inden for de samfundskritiske sektorer).

Forbrugerrådet TÆNK (TÆNK) mener, at certificeringsordningerne bør være obligatoriske, da det vil lette gennemsigtigheden ved sikkerhed i komplekse produkter og bidrage til at samfundet bliver mindre sårbart for cyberangreb. Derudover skal virksomheder ud fra en rimelighedsbetragtning kunne tilbyde forbrugerne produkter med basal ÍT-sikkerhed.

Kommentar
De certificeringsordninger, der bliver vedtaget på europæisk niveau med hjemmel i forordningen, vil som udgangspunkt være frivillige (jf. artikel 56, stk. 2), men der er flere muligheder for at gøre konkrete ordninger obligatoriske. Ordninger kan gøres obligatoriske af både Kommissionen og de enkelte medlemslande, hvis det skønnes nødvendigt. Det bemærkes, at

loven ikke regulerer det konkrete indhold i de kommende certificeringsordninger, herunder spørgsmålet om, hvorvidt ordningen skal være frivillige eller obligatoriske.

3.3. Sammenhæng med øvrige mærkningsordninger

Både DI og TÆNK opfordrer til, at der sikres en form for sammenhæng mellem den mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, som de to organisationer er en del af, og så den kommende europæiske cybersikkerhedscertificeringsordning. Hensynet er, at virksomheder og forbrugere på den måde lettere kan navigere i ordningerne, ligesom en koordineret og sammentænkt indsats må antages at have en mere effektiv indvirkning på cybersikkerheden generelt. DI foreslår endvidere, at der evt. kan oprettes et samarbejde omkring tilsynet med virksomhederne på tværs af mærkningsordningen og de europæiske cybersikkerhedscertificeringsordninger.

Kommentar
Sikkerhedsstyrelsen (SIK) tager kontakt til parterne bag den nye mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse for at afklare mulighederne for et samarbejde, da erfaringer og viden kan være med til at berige og udvikle arbejdet med europæiske certificeringsordninger og omvendt.

Det er dog væsentligt at være opmærksom på, at de europæiske certificeringsordninger og mærkningsordningen for it-sikkerhed og ansvarlig dataanvendelse er meget forskellige.

De europæiske certificeringsordninger, som udstedes som retsakter fra Kommissionen, har fokus på det enkelte produkt, tjeneste eller proces; mens mærkningsordningen har fokus på virksomheden som helhed.

SIKs tilsyn er myndighedsbaseret, mens tilsynet med it-sikkerhed og ansvarlig dataanvendelse har rod i branchen. Forordningen om cybersikkerhed forudsætter, at de organer der skal udstede certifikater, er akkrediteret hertil. Det gør mærkningsordningen ikke.

Selvom det givetvist giver god mening at gå i dialog om en form for samarbejde eller erfaringsudveksling på området, kan de to ordninger derfor for nuværende ikke håndteres under et, ligesom der ikke kan etableres et decideret samarbejde om tilsyn.

SIK er dog som udgangspunkt enig i, at der på EU-niveau bør arbejdes for en ensartet kommunikation, mærkning eller lignende på tværs af de enkelte europæiske certificeringsordninger.

3.4 Adgang til virksomhederne

DI skriver vedrørende Sikkerhedsstyrelsens adgang til virksomhedernes lokaler, som kan ske til enhver tid mod behørig legitimation og uden retskendelse, at det i §13 bør præciseres, at der skal være tale om lokaler, der er relevante for den konkrete certificering.

DI nævner specifikt, at hvis et overensstemmelsesvurderingsorgan udfører andre forretningsaktiviteter på adressen, bør disse lokaler ikke automatisk være omfattet.

Kommentar
Det følger af forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden skal kunne få adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at udføre undersøgelser i overensstemmelse med EU-retten eller medlemsstaternes regler.

Det er dog kun muligt for Sikkerhedsstyrelsen at anvende bestemmelsen i §13 til at tilvejebringe oplysninger til brug for et tilsyn. Det skal således være formålet med adgangen, at der skal indhentes oplysninger, der er nødvendige for selve tilsynet.

Fra andre områder er det SIK's erfaring, at der er behov for, at kontrolmyndighederne – ligesom det er normen på andre områder i dag – kan få adgang til lokaliteter uden retskendelse i de særlige tilfælde, hvor det skønnes nødvendigt. Om det er nødvendigt afhænger således af en proportionalitetsvurdering, herunder om formålet med adgangen kan opnås på anden vis. Der vil i alle tilfælde blive foretaget en konkret vurdering af, om indgrebet er nødvendigt.

3.5 Information til brugerne

Dansk Erhverv & Teleindustrien (DE og TI) anfører, at det skal være muligt at få indsigt i, hvilke produkter, tjenester og processer, som lever op til kravene om at modtage certificeringen.

Forbrugerrådet (TÆNK) skriver, at en frivillig ordning kræver stor velvillighed fra virksomhedernes side - ikke bare i Danmark, men i hele EU - da forbrugerne indkøber og anvender digitale produkter og tjenester på tværs af grænser.

Ifølge TÆNK forpligter det også myndighederne, særligt Sikkerhedsstyrelsen, til at sikre tilstrækkelig information om, hvad certificeringsordningen og et evt. mærke indebærer, sørge for adgang til at se, hvem der har tilsluttet sig ordningen samt oplyse om, hvilke konsekvenser det har at

købe/tilgå ikke-mærkede produkter og tjenester, herunder produkter importeret fra lande uden for EU.

Kommentar
Sikkerhedsstyrelsen vil, evt. i samarbejde med Erhvervsstyrelsen, tilrettelægge en kommunikationsindsats i forbindelse med certificeringsordningernes ikrafttræden. Derudover vil der løbende blive kommunikeret i takt med, at der vedtages certificeringsordninger på EU-niveau.

På EU-niveau bliver der lavet en fælles hjemmeside, hvor man kan få overblik over gældende certificeringsordninger.

3.6. Ensartede definitioner

DE & TI bemærker, at der bør være ensartede definitioner vedrørende cybersikkerhed fra regeringen, så der undgås begrebsforvirring. Konkret nævnes en definition fra den nationale cyber- og informationssikkerhedsstrategi, som DE & TI mener kan opfattes anderledes og mere snævert end rammesætningen i nærværende lovforslag og den bagvedliggende forordning.

Kommentar
Ensartede definitioner er væsentlige for forståelsen af formålet med relevante strategier og lovgivning vedrørende cybersikkerhed.

I det konkrete tilfælde vurderes det, at forståelsen af cybersikkerhed i henholdsvis den nationale cyber- og informationssikkerhedsstrategi og lov om cybersikkerhedscertificering i al væsentlighed er ensartet. Det drejer sig i begge tilfælde om at beskytte systemer og brugere. Forskellen imellem de to begreber er, at brugerne ikke er fremhævet eksplicit i den nationale cyber- og informationssikkerhedsstrategi, men at der her må lægges til grund, at beskyttelse af relevante systemer i sidste ende også handler om at beskytte brugerne.

Det vurderes endvidere at være uhensigtsmæssigt at afvige fra den bagvedliggende definition i forordningen i den lov, der udmønter forordningen nationalt.