FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

8. november 2017

Forslag til Europa-Parlamentets og Rådets forordning om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed") KOM(2017) 477

1. Resumé

Kommissionen fremsatte den 14. september 2017 forslag til forordning om ENISA, "EU's Agentur for Cybersikkerhed", og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed") COM(2017) 477. Forslaget har til formål at sikre et velfungerende indre marked og sørge for et højt niveau af cybersikkerhed, modstandsdygtighed og tillid i EU ved at fastsætte målene og opgaverne for EU's Agentur for cybersikkerhed (ENISA) samt etablere en europæisk ramme for cybersikkerhedscertificering for IKT-produkter og tjenester. Forslaget søger at give ENISA en stærkere og mere central rolle, navnlig ved også at støtte medlemsstaternes gennemførelse af NIS-direktivet, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer, og ved at modvirke trusler på en mere aktiv måde. For at sikre et stabilt grundlag for fremtidig cybersikkerhed tildeles ENISA et permanent mandat, og ENISA's rolle som EU's Agentur for Cybersikkerhed og referencepunkt i EU's cybersikkerhedsøkosystem præciseres. Ydermere skal forslaget om en samlet ramme af regler for indførelsen af specifikke certificeringsordninger bl.a. være med til at øge tilliden til IKT-produkter og -tjenester.

Forslaget forventes at have positive samfundsøkonomiske og erhvervsøkonomiske konsekvenser i kraft af øget cybersikkerhed og et mere velfungerende indre marked gennem styrket tillid og robusthed over for cybersikkerhedstrusler. Forslaget skønnes at have statsfinansielle konsekvenser i kraft af udpegningen af en national tilsynsmyndighed i forbindelse med cybersikkerhedscertificeringsordningen. Forslaget forventes ikke at have lovgivningsmæssige konsekvenser.

Regeringen støtter overordnet set Kommissionens forslag om et nyt, styrket og udvidet mandat til EU's Agentur for Cybersikkerhed (ENISA). Samtidig er det regeringens overordnede holdning, at ENISA's opgaver under ingen omstændigheder bør overskride aktiviteter vedrørende medlemsstaternes nationale sikkerhed og forsvar. Derfor skal der arbejdes hen imod en hensigtsmæssig grænsedragning til spørgsmål af national sikkerhedsmæssig karakter, således at ENISA ikke tildeles operative beføjelser i håndteringen af cyberhændelser.

Endvidere støtter regeringen overordnet forslaget om en fælleseuropæisk ramme for certificering af IKT-produkter og -tjenester. Regeringen lægger vægt på, at der ved udvikling af en ramme for certificeringsordninger skal tilstræbes en balanceret løsning, der både tilgodeser sikkerhedshensyn og virksomheders konkurrence- og vækstvilkår.

2. Baggrund

Kommissionen fremsatte den 14. september 2017 forslag til forordning om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed"). Forslaget er oversendt til Rådet i dansk sprogversion den 11. oktober 2017.

Beskyttelsen af europæerne i den digitale tidsalder blev fremhævet som én af Kommissionens topprioriteter i Jean-Claude Junckers State of the European Union-tale den 13. september 2017, og Kommissionen præsenterede med udgangspunkt heri bl.a. indeværende forordningsforslag om cybersikkerhed samt en ambitiøs meddelelse om opbygning af en stærk cybersikkerhed for EU[1] med det overordnede formål at skabe modstandsdygtighed, afskrækkelse samt at forsvare EU. Meddelelsen bygger videre på de fremskridt, der blev gjort med Kommissionens EU-cyberstrategi fra 2013[2], hvor særligt net- og informationssikkerhedsdirektivet (NIS-direktivet[3]) var et af de store flagskibsinitiativer.

Siden denne første strategi er der sket en yderligere udvikling, herunder det andet mandat for Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA)[4].

I 2016 vedtog Kommissionen en meddelelse[5] om styrkelse af Europas system for modstandsdygtighed over for cyberangreb, hvori der blev bebudet yderligere foranstaltninger til at øge EU-samarbejdets modstandskraft og beredskab.

Disse politiske foranstaltninger og meddelelser blev yderligere styrket af Rådets konklusioner i 2016, som bekræftede, at "ENISA-forordningen er

[1] JOIN(2017) 450 final
[2] JOIN(2013) 1 final
[3] (EU) 2016/1148
[4] (EU) 526/2013
[5] COM(2016) 410 final

et af de centrale elementer i EU's ramme for modstandsdygtighed over for cyberangreb"[6]. I meddelelsen om midtvejsevalueringen af strategien for det digitale indre marked fra maj 2017[7] angav Kommissionen, at den ville revidere ENISA's mandat senest i september 2017. Dette skulle ske for at definere ENISA's rolle i det ændrede IT-sikkerhedsøkosystem.

3. Formål og indhold

Forordningsforslaget har til formål at sikre et velfungerende indre marked med et højt niveau af cybersikkerhed, modstandsdygtighed og tillid i EU ved at fastsætte målene og opgaverne for EU's Agentur for Cybersikkerhed, ENISA, samt etablere en fælleseuropæisk ramme for cybersikkerhedscertificering for produkter og tjenester inden for informations- og kommunikationsteknologi (IKT).

ENISA – EU's Agentur for Cybersikkerhed
Forslaget søger at give ENISA en stærkere og mere central rolle, navnlig ved også at støtte medlemsstaternes gennemførelse af NIS-direktivet og ved at modvirke trusler på en mere aktiv måde. I henhold til forslaget tildeles ENISA et permanent mandat for at sikre et stabilt grundlag for fremtiden, og ENISA's rolle som EU's Agentur for Cybersikkerhed og referencepunkt i EU's cybersikkerhedsøkosystem præciseres.

Forordningsforslaget lægger således op til, at ENISA skal varetage nedenstående centrale opgaver.

Udvikling og implementering af EU-politikker og regulering
ENISA får til opgave at bidrage proaktivt til udviklingen af politik i forhold til net- og informationssikkerhed samt andre politiske initiativer med cybersikkerhedselementer inden for forskellige sektorer (f.eks. energi, transport og finans). ENISA vil i denne forbindelse få en styrket rådgivende rolle, herunder i form af uafhængige vurderinger og forberedende arbejde til udvikling og ajourføring af politikker og lovgivning.

Det er desuden hensigten, at ENISA skal støtte medlemsstaterne i forbindelse med implementeringen af NIS-direktivet, der har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer inden for en række særligt samfundsvigtige sektorer (energi, transport, bankvæsen, sundhed, drikkevandsforsyning, digital infrastruktur mv.). Effektiv implementering vil således sikre et bredt samfundsmæssigt løft af cyber- og informationssikkerheden. I forbindelse med implementering af NIS-direktivet, vil ENISA skulle bistå medlemsstaterne med at opnå en ensartet tilgang for så vidt angår gennemførelsen af direktivet på tværs af grænser og sektorer. Ligeledes vil ENISA skulle støtte arbejdet i Samarbejdsgruppen, som har til opgave at støtte medlemsstaterne i implementeringen af NIS-

[6] Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri – 15. november 2016. (Dok. 14540/16)
[7] COM(2017) 228 final

direktivet samt at understøtte strategisk samarbejde mellem medlemsstaterne.

Med det formål at understøtte den regelmæssige revision af politikker og lovgivning på cybersikkerhedsområdet vil ENISA endvidere skulle foretage regelmæssige indberetninger om status for gennemførelsen af EU's retlige rammer, herunder vedrørende medlemsstaternes anmeldelser af hændelser til samarbejdsgruppen via de centrale kontaktpunkter i henhold til artikel 10, stk. 3, i NIS-direktivet.

ENISA vil ligeledes få til opgave at understøtte EU's politikker og lovgivning inden for området elektronisk kommunikation og elektroniske identifikations- og tillidstjenester med sigte på at fremme et højere cybersikkerhedsniveau.

Kapacitetsopbygning
ENISA får til opgave at bidrage til at forbedre EU's og de nationale offentlige myndigheders kapacitet og ekspertise, herunder i forbindelse med håndtering af hændelser og gennemførelse af lovgivningsmæssige foranstaltninger indenfor cybersikkerhed. I denne forbindelse vil ENISA fortsat skulle tilrettelægge årlige cybersikkerhedsøvelser på EU-plan. Agenturet vil ligeledes skulle bidrage til etableringen af centre for informationsudveksling og analyse (ISAC'er) inden for en række sektorer ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer til rådighed.

Operationelt samarbejde og krisestyring
Med forslaget bemyndiges ENISA til at understøtte det operationelle samarbejde på tværs af EU's institutioner og på tværs af medlemsstaterne, herunder i CSIRT-netværket som udgøres af medlemsstaternes CSIRT'er (Computer Security Incident Response Team) i medfør af NIS-direktivet. I denne forbindelse vil ENISA indgå i et struktureret samarbejde med CERT-EU (EU's Computer Emergency Response Team).

I tilfælde af større grænseoverskridende cybersikkerhedshændelser eller -kriser, og med det formål at fremme operationelt samarbejde, foreslås ENISA bemyndiget til at:

a) sammenstille rapporter fra nationale kilder med henblik på at bidrage til at skabe en fælles situationsforståelse;
b) sikre en effektiv informationsstrøm og sørge for, at der er eskalationsmekanismer på plads til brug mellem CSIRT-netværket og de tekniske og politiske beslutningstagere på EU-niveau;
c) understøtte den tekniske håndtering af en hændelse, herunder ved at fremme delingen af tekniske løsninger mellem medlemsstaterne;
d) understøtte kommunikation til offentligheden om en hændelse; og
e) afprøve samarbejdsplaner for reaktionen på væsentlige hændelser.

Efter anmodning fra to eller flere berørte medlemsstater og alene med det formål at levere rådgivning om forebyggelse af fremtidige hændelser vil ENISA endvidere kunne yde støtte til eller foretage en efterfølgende teknisk undersøgelse af hændelser med betydelig eller væsentlig virkning i henhold til NIS-direktivet. ENISA vil ligeledes kunne foretage en sådan undersøgelse

efter anmodning fra Kommissionen og efter aftale med de berørte medlemsstater i tilfælde, hvor flere end to medlemsstater berøres af en hændelse.

Endelig vil ENISA få til opgave regelmæssigt at udarbejde en teknisk EU-cybersikkerhedsrapport om hændelser og trusler, der skal være baseret på offentligt tilgængelige oplysninger, ENISA's egen analyse samt rapporter, som på frivillig basis deles af bl.a. medlemsstaternes CSIRT'er eller NIS-direktivets centrale kontaktpunkter (jf. artikel 14, stk. 5, i NIS-direktivet), Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol eller CERT-EU.

Markedsrelaterede opgaver
ENISA vil få til opgave at understøtte det indre marked, herunder ved at analysere udviklingstendenser på cybersikkerhedsmarkedet og ved at understøtte EU's politikudvikling inden for IKT-standardisering og IKT-cybersikkerhedscertificering.

Viden, information og oplysning
ENISA skal være EU's informationsknudepunkt vedrørende net- og informationssikkerhed. Det indebærer fremme og udveksling af bedste praksis og initiativer på tværs af EU. Agenturet vil ligeledes skulle stille rådgivning, vedledning og bedste praksis vedrørende sikkerheden af kritiske infrastrukturer til rådighed. Efter en væsentlig grænseoverskridende hændelse vil ENISA desuden få til opgave at udarbejde rapporter med henblik på at give vejledning til virksomheder og borgere i hele EU på baggrund af den pågældende hændelse.

Forskning og innovation
ENISA får til opgave at rådgive EU og nationale myndigheder om fastsættelse af prioriteter indenfor forskning og udvikling på cyberområdet, herunder også i sammenhæng med det kontraktlige offentlig-private partnerskab vedrørende cybersikkerhed. ENISA's rådgivning om forskning skal ligeledes bidrage til det nye europæiske forsknings- og kompetencecenter for cybersikkerhed under den næste flerårige finansielle ramme. Endelig vil ENISA – efter anmodning fra Kommissionen – blive involveret i gennemførelsen af EU's finansieringsprogrammer inden for forskning og innovation på cyberområdet.

Internationalt samarbejde
Endelig vil ENISA få til opgave at bidrage til EU's indsats for at fremme internationalt samarbejde om cybersikkerhed ved at deltage som observatør og i tilrettelæggelsen af internationale øvelser, på Kommissionens anmodning at fremme udveksling af bedste praksis mellem relevante internationale organisationer samt efter anmodning at stille ekspertise til rådighed for Kommissionen.

Fælles europæisk ramme for cybersikkerhedscertificering for IKT-produkter og tjenester

Forslaget indfører ikke direkte operationelle certificeringsordninger, men etablerer i stedet en samlet ramme af regler for indførelsen af specifikke europæiske certificeringsordninger for IKT-produkter og -tjenester, der udarbejdes af ENISA og vedtages ved gennemførelsesretsakter jf. proceduren beskrevet neden for.

Certificeringsordninger
En cybersikkerhedscertificeringsordning vil i henhold til forslaget attestere, at de pågældende IKT-produkter og -tjenester, der er certificeret i overensstemmelse med ordningen, opfylder de nærmere fastsatte cybersikkerhedskrav. Det gælder f.eks. i forhold til deres evne til at beskytte mod kompromittering af tilgængeligheden, autenticiteten, integriteten og fortroligheden af de data, der opbevares eller behandles i produktet eller tjenesten. De europæiske certificeringsordninger vil ikke selv udvikle tekniske standarder, men i stedet gøre brug af eksisterende standarder i relation til de tekniske krav og evalueringsprocedurer, som produkterne konkret skal overholde.

De konkrete cybersikkerhedscertificeringsordninger skal udformes så de alt efter relevans for produkt- eller tjenestegruppen tager hensyn til en række sikkerhedsmål, herunder at:

- beskytte data mod utilsigtet eller uautoriseret behandling eller ødelæggelse;
- sikre, at kun autoriserede personer, programmer eller maskiner har adgang til data;
- genetablere tilgængelighed af og adgang til data i tilfælde af fysiske eller tekniske hændelser;
- sikre, at IKT-produkter og -tjenester er forsynet med ajourført software.

Forslaget indebærer endvidere, at ordningerne skal fastsætte en række specifikke elementer, der angiver omfanget og indholdet af cybersikkerhedscertificeringen. Det omfatter blandt andet udpegning af de omfattede produkter og tjenester, nærmere specifikation af cybersikkerhedskravene (f.eks. med henvisning til relevante standarder eller tekniske specifikationer), de specifikke evalueringskriterier og -metoder og det tillidsniveau, de påtænkes at garantere (det vil sige grundlæggende, betydeligt eller højt).

Forberedelse og vedtagelse af certificeringsordninger
Det følger af forslaget, at de europæiske certificeringsordninger udarbejdes af ENISA med bistand fra og i tæt samarbejde med en europæisk cybersikkerhedscertificeringsgruppe, der skal nedsættes med forordningen (jf. nedenfor). Det vil være Kommissionen, der vedtager certificeringsordningerne ved hjælp af gennemførelsesretsakter. Endvidere er det i henhold til forslaget Kommissionen, der igangsætter arbejdet med en given certificering ved at anmode ENISA om at udarbejde en ordning for specifikke IKT-produkter eller -tjenester.

Cybersikkerhedscertificering
Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenter og udbydere af IKT-tjenester indgive en ansøgning om certificering af deres produkter eller tjenester. Certificeringen er i henhold til forslaget frivillig, medmindre andet er fastsat i EU-retten.

Certificering og udstedelse af cybersikkerhedsattesten skal foretages af overensstemmelsesvurderingsorganer, der er akkrediteret til at foretage certificeringer. Akkrediteringen foretages således af de nationale akkrediteringsorganer, der er udpeget i henhold til forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter. I Danmark er dette Den Danske Akkrediteringsfond (DANAK). I undtagelsestilfælde kan det efter forslaget fastsættes i en certificeringsordning, at certificeringen i behørigt begrundede tilfælde skal foretages af et offentligt organ. De nationale tilsynsmyndigheder skal for hver europæisk certificeringsordning underrette Kommissionen om de akkrediterede overensstemmelsesvurderingsorganer. Kommissionen vil på baggrund heraf et år efter ikrafttrædelsen af forslaget skulle offentliggøre en liste over de anmeldte overensstemmelsesvurderingsorganer.

Cybersikkerhedsattesterne udstedes for en periode på højst tre år og vil kunne forlænges på samme vilkår, hvis de relevante krav fortsat er opfyldt. En europæisk cybersikkerhedsattest skal anerkendes i alle medlemsstater.

Nationale cybersikkerhedscertificeringsordninger
Nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der bliver omfattet af en europæisk certificeringsordning, vil i henhold til forslaget ophøre med at have virkning. Det vil ske fra det tidspunkt, der fastsættes i den gennemførelsesretsakt, hvorved ordningen vedtages. Formålet er at sikre harmonisering og undgå fragmentering af det indre marked. Medlemsstaterne må i forlængelse heraf heller ikke vedtage nye nationale certificeringsordninger for IKT-produkter og -tjenester, der i forvejen er omfattet af en europæisk ordning. Allerede udstedte attester i henhold til en national certificeringsordning forbliver dog gyldige indtil deres udløbsdato.

Myndighedstilsyn
I henhold til forslaget skal medlemsstaterne sørge for, at der er en myndighed, som fører tilsyn med certificeringen, herunder at overensstemmelsesvurderingsorganerne overholder reglerne, og at de attester, som organerne udsteder, er i overensstemmelse med de krav, der følger af henholdsvis forordningen og den tilsvarende europæiske cybersikkerhedscertificeringsordning. Den nationale certificeringstilsynsmyndighed skal endvidere i henhold til forslaget kunne behandle klager i forbindelse med attester udstedt af overensstemmelsesvurderingsorganerne. Endelig skal tilsynsmyndigheden samarbejde med andre eksisterende nationale certificeringstilsynsmyndigheder eller andre offentlige myndigheder f.eks. i forhold til informations-

udveksling om mulige tilfælde, hvor IKT-produkter og -tjenester ikke overholder reguleringen.

Den europæiske cybersikkerhedscertificeringsgruppe
I henhold til forslaget skal der etableres en europæisk cybersikkerhedscertificeringsgruppe, der består af alle medlemsstaters nationale certificeringstilsynsmyndigheder. Gruppen får som sin vigtigste opgave dels at rådgive Kommissionen om problemstillinger vedrørende cybersikkerhedscertificeringspolitik og dels at samarbejde med ENISA om udarbejdelsen af udkast til europæiske cybersikkerhedscertificeringsordninger. Gruppen har endvidere med forslaget mulighed for at foreslå Kommissionen, at den anmoder ENISA om at udarbejde et forslag til certificeringsordning. Det vil være Kommissionen, der varetager formandskabet og sekretariatsfunktionen for gruppen med bistand fra ENISA.

Sanktioner
Medlemsstaterne skal i henhold til forslaget fastsætte regler for sanktioner for overtrædelse af forordningens bestemmelser og de europæiske certificeringsordninger. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Øvrige bestemmelser
Udvalgsprocedure
Efter forslaget er vedtaget, skal der nedsættes et udvalg i overensstemmelse med komitologiforordningen ((EU) 182/2011). Udvalget skal bistå Kommissionen i udarbejdelsen af de gennemførelsesretsakter, der henvises til under afsnittet om den europæiske ramme for cybersikkerhedscertificeringsordninger.

Ikrafttræden
Efter forslagets vedtagelse træder forordningen i kraft 20 dage efter offentliggørelse i Den Europæiske Unions Tidende.

Evaluering
Efter forslagets vedtagelse skal Kommissionen hvert femte år vurdere virkningen af ENISA's arbejde, herunder eventuelle behov for at ændre agenturets mandat. Evalueringen skal også omfatte virkningen af certificeringsordningen i forhold til målene om at sikre tilstrækkelig cybersikkerhed i IKT-produkter og forbedre det indre markeds funktion.

4. Europaparlamentets udtalelser

Der foreligger endnu ikke en udtalelse fra Europaparlamentet.

5. Nærhedsprincippet

Det er Kommissionens opfattelse, at forordningsforslaget er i overensstemmelse med nærhedsprincippet. Under henvisning til net- og informationssikkerheds grænseoverskridende karakter fremhæver Kommissionen, at individuelle tiltag fra enkelte medlemsstater og en fragmenteret tilgang til cyber-

sikkerhed ikke er tilstrækkeligt for at øge den kollektive robusthed. Målet med forslaget kan således ikke i tilstrækkelig grad opfyldes af medlemsstaterne alene og nås derfor bedre på EU-plan.

Regeringen er på det foreliggende grundlag enig i Kommissionens vurdering og finder således, at nærhedsprincippet er overholdt, da cybersikkerhedstrusler i sagens natur er grænseoverskridende.

6. Gældende dansk ret

ENISA og cybersikkerhedscertificeringsordninger er ikke i dag reguleret af dansk lovgivning.

7. Konsekvenser

Lovgivningsmæssige konsekvenser
Kommissionen har fremsat forslag til en forordning, der ikke skal implementeres, men vil gælde umiddelbart i medlemslandene. Vedtagelse af forslaget vurderes ikke at have yderligere lovgivningsmæssige konsekvenser.

Økonomiske konsekvenser
Statsfinansielle konsekvenser
Vedtagelse af den del af forslaget, der vedrører ENISA's opgaver og organisatoriske forhold, vurderes at kunne få statsfinansielle konsekvenser i form af konsekvenser for EU's budget.

For så vidt angår forslagets bestemmelser om en europæisk ramme for cybersikkerhedscertificeringsordninger vil udpegningen af en national tilsynsmyndighed kunne have statsfinansielle konsekvenser. Omfanget af disse kan imidlertid ikke vurderes på nuværende tidspunkt.

Samfundsøkonomiske konsekvenser
Det er forventningen, at vedtagelsen af forslaget vil føre til et højere niveau af cybersikkerhed, modstandsdygtighed og tillid i EU gennem øget kapacitet, samarbejde, risikostyring og bevidsthed om cybersikkerhed. Dette kan være med til at forbedre det indre markeds funktion samt bidrage til udviklingen af et digitalt indre marked gennem styrket tillid og robusthed over for cybersikkerhedstrusler. Forslaget vurderes på denne baggrund at kunne have positive samfundsøkonomiske konsekvenser.

Erhvervsøkonomiske konsekvenser
ENISA's opgaver og organisatoriske forhold forventes ikke i sig selv at medføre administrative konsekvenser for erhvervslivet i Danmark. Dog vil ENISA's udvidede beføjelser på baggrund af forordningsforslaget på længere sigt kunne medføre administrative konsekvenser for erhvervslivet. Omfanget af disse kan imidlertid ikke vurderes på nuværende tidspunkt.

Etableringen af en europæisk ramme for cybersikkerhedscertificeringsordninger forventes umiddelbart at medføre positive erhvervsøkonomiske konsekvenser for danske virksomheder. Forslaget vurderes således at forbedre

mulighederne for at drive virksomhed på tværs af grænserne og indrette forretningen mere effektivt.

Andre konsekvenser og beskyttelsesniveauet
En vedtagelse af forslaget skønnes ikke at berøre beskyttelsesniveauet i Danmark.

8. Høring

Forslaget har været i høring i Specialudvalget for Energi-, Forsynings- og Klimapolitik og EU-specialudvalget for Konkurrenceevne, vækst og forbrugerspørgsmål med frist for bemærkninger den 3. oktober 2017. Der er modtaget høringssvar fra Dansk Industri, TDC Group, Finans Danmark, Dansk Erhverv, Ingeniørforeningen, IDA, KL, Teleindustrien (TI), Dansk Standard (DS) samt Dansk Byggeri.

Generelle bemærkninger
Finans Danmark bemærker overordnet, at den øgede digitalisering betyder, at cybersikkerhed er særdeles vigtig for bankerne. Dertil er omfanget, kompleksiteten og hastigheden i de internationale såvel som de nationale cybertrusler for massive og vedholdende til, at én part kan løfte udfordringerne alene. Derfor er et samarbejde mellem det offentlige og det private og en inddragelse af borgerne afgørende. Nationale grænser skal ikke være en hindring for effektiv bekæmpelse af grænseoverskridende cyberkriminalitet. På den baggrund ser Finans Danmark Kommissionens forslag om ENISA og cybersikkerhedscertificering som et positivt initiativ til at styrke den europæiske cybersikkerhed. Cybersikkerhedscertificering kan blandt andet bidrage til at håndtere udfordringen med IoT (Internet of Things). Finans Danmark anbefaler, at en europæisk certificeringsmodel funderes på globalt anerkendte standarder.

Ingeniørforeningen, IDA er overordnet set meget positiv over for at styrke indsatsen for cybersikkerhed i Europa. De påpeger, at en koordineret indsats, der involverer alle EU lande, er en fordel og en nødvendighed. Det er dog nødvendigt, at en sådan indsats får den nødvendige slagkraft i form af ressourcer og kompetencer.

Ingeniørforeningen bemærker desuden, at der i annekset til forslaget nævnes, at overensstemmelsesorganer skal have en juridisk profil og muligheden for at trække på tekniske kompetencer. Ingeniørforeningen vil her anbefale, at der i annekset henvises til "legal and technical personality". Hvis en sådan enhed skal have den nødvendige slagkraft, kræver det dedikerede tekniske ressourcer som en fast del af organisationen. Vidensopbygning og erfaring er centralt, hvis initiativet i sig selv skal få effekt og hvis en sådan enhed skal have opnå legitimitet og den styrkede branding, man ønsker.

TDC Group forventer, at Kommissionens forslag vil styrke EU's kapacitet til at respondere, dele bedste praksis og udvikle videndeling-platforme til at håndtere cybersikkerhed.

ENISA – EU's Agentur for Cybersikkerhed
Overordnet set støtter Dansk Erhverv, Dansk Industri, Finans Danmark, Teleindustrien og TDC Group forslagets formål om et styrket cybersikkerhedsagentur med et permanent mandat, som et vigtigt initiativ til at højne den europæiske cybersikkerhed, dog med visse bemærkninger.

Med reference til den stigende og grænseoverskridende cybertrussel, påpeger Dansk Erhverv nødvendigheden af, at myndigheder på tværs af EU arbejder sammen, også i forhold til opbygning af mere kompetence, opmærksomhed og forskning på området. Her ønsker Dansk Erhverv særligt at komplimentere, at ENISA skal udbyde vejledning på bedste praksis for individuelle brugere, hvilket Dansk Erhverv ser som en styrkelse af opmærksomheden om cyber-hygiejne, som anses for at være centralt for at øge cybersikkerheden i EU. I denne sammenhæng understreger Dansk Erhverv imidlertid, at sådanne bedste praksis bør være baseret på metoder, der har været anvendt med succes i nogle lande, og ikke blot er baseret på teori. Dansk Erhverv hilser det ligeledes velkomment, at der sættes fokus på internationalt samarbejde med andre internationale organisationer om cybersikkerhed, idet cyberkriminalitet anses for værende et globalt fænomen. Endelig understreger Dansk Erhverv vigtigheden af, at ENISA får ressourcer nok til at tiltrække de mest velkvalificerede medarbejdere, hvis agenturet skal kunne løfte disse nye opgaver på tilstrækkelig vis.

Dansk Industri understreger væsentligheden af at sikre, at der, i etableringen af et permanent mandat til ENISA, sker en organisatorisk klarhed i EU's håndtering af spørgsmål relateret til cybersikkerhed, således at myndigheder og virksomheder alene skal orientere sig mod ét sted i EU. Samtidig lægger Dansk Industri vægt på, at imødegåelse af cybertrusler ikke alene er et europæisk anliggende, og understreger, at det, i processen mod konsolidering af EU's indsats til imødegåelse af cybertrusler, er afgørende, at der fortsat er fokus på samarbejde med øvrige internationale samarbejdspartnere.

Teleindustrien støtter forslaget om oprettelse af et cybersikkerhedsagentur og lægger i den forbindelse vægt på, at det sikres, at arbejdet i agenturet i høj grad koncentreres omkring dialog og samarbejde mellem offentlige og private aktører for at sikre et højt sikkerhedsniveau.

TDC Group understreger nødvendigheden af et styrket cybersikkerhedsagentur for at udfylde målsætningerne i NIS-direktivet og sikre bedre samarbejde mellem nationale cybersikkerhedsmyndigheder. TDC Group fremhæver, at forslaget særligt kan gavne mindre lande, idet myndighederne i disse lande må forventes at have særlig stor gavn af sparring og indhentning af viden fra et styrket agentur. TDC Group ser gerne, at ENISA fortsætter traditionen med at føre dialog med både myndigheder og privatsektoren, idet både offentlige og private aktører er nødvendige i forhold til at sikre optimal cybersikkerhed.

KL anbefaler, at der sker en tæt koordinering af de nationale aktiviteter mod cyberkriminalitet med aktiviteterne i ENISA, bl.a. med henblik på at sikre koordinerede processer for indsamling af information om sikkerhedsbrud, og gør i denne sammenhæng opmærksomme på et særligt initiativ i

den fællesoffentlige digitaliseringsstrategi for 2016-2020, som skal sikre, at offentlige myndigheder arbejder efter konkrete sikkerhedstiltag for at imødegå trusler om hacking. KL har desuden noteret sig, at ENISA vil tilbyde offentlige myndigheder træning i cybersikkerhed, jf. artikel 6, stk. 1, litra h, samt organisere større, årlige cybersikkerhedsøvelser, jf. artikel 6, stk. 1, litra g. KL vil ligeledes anbefale, at der sker en national koordinering af disse aktiviteter.

Fælles europæisk ramme for cybersikkerhedscertificering for IKT-produkter og tjenester

Dansk Erhverv, Dansk Industri, Finans Danmark, Ingeniørforeningen IDA, Dansk Standard, Teleindustrien, TDC Group, støtter endvidere overordnet forslaget om indførelse af en fælleseuropæisk ramme for cybersikkerhedscertificering.

Dansk Erhverv hilser det ligeledes velkomment, at Kommissionen har valgt at fremsætte et forslag til et frivilligt certificeringssystem i EU. Dansk Erhverv vurderer, at det er en afbalanceret tilgang til problemstillingen, og understreger vigtigheden af, at certificeringerne er virksomhedsdrevne og udarbejdes i tæt samarbejde med erhvervslivet. Dansk Erhverv udtrykker tilfredshed med fleksibiliteten i forslaget, herunder at mærkning af produkter kan være en del af certificeringen, hvor industrien mener det giver mening, men ikke er et fast kriterie. Dansk Erhverv hilser det ligeledes velkomment, at forslaget skitserer tre forskellige niveauer af beskyttelse med forskellige kriterier, hvilket gør det muligt for virksomheder at tilpasse certificeringen den risiko, som produktet udgør. Dette kan bidrage til sikkerhed i balance. Dansk Erhverv betragter det desuden som positivt og meget vigtigt, at der lægges op til, at EU-certificeringer udarbejdes i overensstemmelse med internationale standarder og certificeringer, således at dobbeltregulering undgås, og EU certificeringerne ikke fører til handelsbarrierer. Dansk Erhverv vurderer endvidere, at forslagets krav om, at EU-certificeringer skal anerkendes i alle medlemslande er helt essentielt og kan bidrage til at nedbringe omkostningerne for certificering for SMVer og Start-ups – og gøre det lettere for dem at benytte sig af det indre marked, da de kun vil have behov for én certificering i stedet for forskellige i forskellige medlemslande. Dette er positivt, men for at denne gevinst skal kunne realiseres vurderer Dansk Erhverv det for nødvendigt, at EU-certificeringsmekanismen ikke bliver for tung, og at det hele tiden holdes for øje, at den skal være anvendelig også for små virksomheder.

Dansk Industri har samme grundlæggende holdning i forhold til Kommissionens forslag til cybersecurity-certificering af Informations- og Kommunikationsteknologi som til etableringen af et permanent mandat til ENISA. En europæisk certificeringsmodel skal således være globalt orienteret og funderet, så der ikke skabes hindringer for handel med resten af verden. Det vil sige, at arbejdet så vidt muligt baseres på globalt anerkendte metoder og standarder. Endelig lægger Dansk Industri vægt på, at certificeringsgrundlaget etableres i et samarbejde med erhvervslivet, så kriterierne i standardiseringsarbejdet så vidt muligt tager højde for den markedsdrevne udvikling.

For så vidt angår standarder og cybersikkerhedscertificering bemærker Ingeniørforeningen, at det er vigtigt, at en yderligere indsats på standarder

for cybersikkerhed og privacy er yderst vigtigt, men at EU's rolle i denne sammenhæng bør være at bakke op om de initiativer, der allerede foregår i de traditionelle standardiseringsnetværk. Ingeniørforeningen påpeger, at både CEN/CENELEC og ETSI har som europæiske standardiseringsorganisationer en proces, der sikrer deltagelse og høringsmulighed for både myndigheder, virksomheder, forskere og civilsamfund, herunder også en indsats for at inddrage små og mellemstore virksomheder bedst muligt. Ingeniørforeningen er endvidere meget positiv over for en cybersikkerhedscertificering af IKT produkter og tjenester, Idet det kan være uoverskueligt for især mindre virksomheder at overskue, hvad der er sikker teknologiimplementering og det må derfor anses for en væsentlig hjælp, at der findes myndighedsgodkendte certificeringer at rette sig efter. For virksomheder, der producerer f.eks. robotter og it-systemer, vil EU-harmoniserede certificeringer hjælpe til at kunne nå flere markeder uden at skulle tilrette vidt forskellige krav.

Dansk Standard finder det relevant, at der etableres en fælleseuropæisk ramme for cybersikkerhedscertificering, som kan give virksomheder mulighed for at certificere produkter og dermed bidrage til tryghed og sikkerhed hos kunderne. Dansk Standard finder det også vigtigt at etablere en fælles europæisk certificeringsmodel, så man undgår, at det samme produkt skal certificeres på forskellige måder i forskellige EU medlemslande, som det er tilfældet i dag i Tyskland, Frankrig og UK. For Dansk Standard er det afgørende, at den foreslåede europæiske certificeringsmodel bygger på relevante standarder, der sikrer et effektivt beskyttelsesniveau og så vidt muligt bruger globalt anerkendte standarder. Det er også vigtigt certificeringsmodellen ikke skaber hindringer for samhandel mellem EU og resten af verden. Dansk Standard bemærker endvidere, at udvikling af standarder, som skal understøtte europæisk politik og regulering foregår gennem de europæiske standardiseringsorganisationer CEN/CENELEC og ETSI. Disse organisationer sikrer europæiske aktører adgang til at deltage og påvirke udviklingen af standarder. Dansk Standard foreslår, at arbejdet med at udvikle og udvælge standarder til brug for en europæisk certificeringsmodel forankres i CEN/CENELECs tekniske komité, der skal arbejde med cybersikkerhed og databeskyttelse (CEN TC 13), og at der etableres et tæt samarbejde med Kommissionen og ENISA herom. Det vil betyde at grundlaget for certificeringen kan udvikles gennem en transparent proces, hvor virksomheder og andre europæiske interessenter har mulighed for at deltage og bidrage til kriterierne for certificeringsordningen med den nyeste viden på markedet. Vælger man en model, hvor kriterierne fastlægges udelukkende af myndigheder, kan man ikke drage fordel af den viden der er i markedet og man risikerer at pålægge virksomhederne unødige byrder.

Teleindustrien støtter endvidere forslaget om fælles standarder for EU certificering af informations- og kommunikationsteknologi. Fælles standarder for eksempelvis teleudstyr på tværs af EU vil bidrage til at sikre et fælles niveau for sikkerhed og lige konkurrencevilkår på tværs af lande i EU.

TDC Group støtter op om forslaget vedr. fælles standarder for EU certificering af informations- og kommunikationsteknologi. Paneuropæiske standarder ville gavne markedet for ydelser fra underleverandører, som i dag er udsat for fragmenterede krav på tværs af EU lande. Dette præsenterer væ-

sentlige byrder og omkostninger for leverandørerne, som ville drage store fordele af at leve op til konsoliderede europæiske standarder. TDC Group ser især et stort potentiale på leverancer af kritisk infrastruktur, og ønsker at understrege at både europæiske og ikke-europæiske leverandører skal have mulighed for at opnå certificering, for at sikre et mangfoldigt og konkurrencedygtigt marked for disse tjenester. TDC Group finde det i forlængelse heraf nødvendigt at få afklaret de konkrete omstændigheder omkring afprøvelse og certificering, herunder hvilken overgangsordning myndigheder vil indføre i relation til fortsat drift af eksisterende udstyr, som endnu ikke er certificeret, når EU bestemmelserne træder i kraft.

KL vil af resursehensyn anbefale, at det i forhold til forslaget om en cybersikkerhedscertificeringsordning overvejes, hvorvidt ordningen, – i det omfang den vil være relevant for offentlige myndigheder – kan samtænkes med mulighederne for databeskyttelsescertificering efter databeskyttelsesforordningen (2016/679).

9. Generelle forventninger til andre landes holdninger

Mange medlemsstater har udtrykt støtte til at styrke ENISA, herunder at ENISA tildeles et permanent mandat. Der hersker imidlertid bred skepsis blandt medlemsstaterne over for Kommissionens forslag om at styrke agenturets operationelle rolle.

Mange medlemsstater har desuden udtrykt generel støtte til forslaget om en fælleseuropæisk certificeringsramme for IKT-produkter, og bl.a. lagt vægt på, at det kan bidrage til at styrke tilliden til digitale produkter og tjenesteydelser – og dermed øge muligheden for at drage fordel af det digitale indre marked. Samtidig har flere medlemsstater understreget vigtigheden af, at en certificeringsramme ikke bliver unødigt byrdefuld for virksomhederne, særligt SMV'er, og at der bliver forskellige grader af sikkerhedscertificering afhængigt af, hvilken type IKT-produkt eller -tjenesteydelse, det drejer sig om.

10. Regeringens foreløbige generelle holdning

Regeringen støtter overordnet Kommissionens forslag om et nyt, styrket og udvidet mandat til EU's Agentur for Cybersikkerhed (ENISA) samt et fælleseuropæisk IKT-certificeringssystem.

Det er regeringens foreløbige, generelle holdning, at der er behov for et styrket europæisk cybersikkerhedsagentur med et permanent mandat, som skal sikre kapacitetsopbygning, videndeling, forskning og innovation, opmærksomhed og samarbejde på tværs af EU. Dette skal ikke mindst ses i lyset af cybersikkerheds grænseoverskridende karakter. Således er det væsentligt at sikre samordning i tilgangen til cybersikkerhed på tværs af EU for at styrke den kollektive robusthed mod cyberangreb.

Samtidig er det regeringens overordnede holdning, at ENISA's opgaver ikke bør overskride aktiviteter vedrørende medlemsstaternes nationale sikkerhed og forsvar. Regeringen lægger vægt på, at medlemsstaternes rolle og ansvar for egen cybersikkerhed og modsvar til cybertrusler fastholdes. Der

skal således arbejdes henimod en hensigtsmæssig grænsedragning til spørgsmål af national sikkerhedsmæssig karakter.

Det er derfor regeringens overordnede holdning, at ENISA ikke skal tildeles operative beføjelser i håndteringen af cyberhændelser, herunder særligt, at ENISA ikke bør bemyndiges til at skabe en fælles situationsforståelse eller understøtte teknisk håndtering og deling af tekniske løsninger mellem medlemsstaterne. Regeringen har fokus på, at fx klassificerede oplysninger skal behandles særskilt og i overensstemmelse med national lovgivning og national sikkerhed. Dette skyldes bl.a., at der kan være operative og/eller sikkerhedsmæssige hensyn. Det bemærkes i denne sammenhæng, at det ligeledes er regeringens overordnede holdning, at operationelt samarbejde mellem medlemsstaterne, herunder etableringen af fælles situationsforståelse, teknisk håndtering og deling af tekniske løsninger, skal faciliteres igennem CSIRT-netværket, som er oprettet i medfør af NIS-direktivet.

Regeringen støtter overordnet forslaget om en fælleseuropæisk ramme for certificering af IKT-produkter og -tjenester. Regeringen lægger dog vægt på, at udviklingen af en ramme for certificeringsordninger både skal tilgodese sikkerhedshensyn og virksomheders konkurrence- og vækstvilkår. Det er i denne sammenhæng vigtigt, at en ramme for certificeringsordninger indføres på lige, objektive og ikke-diskriminerende vilkår. Det digitale område er et område, hvor udviklingen går stærkt og eventuelle krav om certificering skal derfor være fleksible og fremtidssikrede, så konkurrencen ikke forvrides unødigt eller hæmmer innovationen på området.

Regeringen arbejder for, at certificeringssystemet bliver lettilgængeligt og anvendeligt for alle virksomheder, herunder små og mellemstore virksomheder samt iværksættere. Endvidere lægger regeringen vægt på, at medlemsstaterne og alle relevante interessenter inddrages i arbejdet med fælleseuropæiske certificeringsordninger, herunder ift. delegerede retsakter og gennemførelsesretsakter, og at der i vidt omfang tages udgangspunkt i eksisterende europæiske og internationale standarder samt tages højde for behovet for udviklingen af nye standarder.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.