ERHVERVSMINISTERIET

NOTAT

15. november 2018
18/09069-1
mgl-dep

Rådsmøde (transport, telekommunikation og energi) den 3-4. december 2018.

Indhold

Kommissionens forslag til en forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre, KOM(2018) 630.

Notat er en opdatering af grund- og nærhedsnotat af 12. oktober 2018. Ændringerne er fremhævet med ***fed/kursiv***.

1. Resumé

*Kommissionen har fremlagt et forslag til forordning om etablering af et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og et netværk af nationale koordinationscentre. Formålet med forslaget er at bevare og udvikle teknologiske og industrielle kapaciteter vedrørende cybersikkerhed, øge den europæiske cybersikkerhedsindustris konkurrenceevne og gøre cybersikkerhed til en konkurrencemæssig fordel for andre industrier i EU. Forslagets ventes at få væsentlige statsfinansielle konsekvenser. EU-**budgettet**s bidrag til det europæiske kompetencecenter vil jf. forslaget udgøre 1.981.668.000 euro **(løbende priser)** i perioden 2021-27 fra programmet for Det Digitale Europa samt et endnu ikke fastsat beløb fra Horisont Europa-programmet. Deltagende medlemsstater vil ydermere skulle yde et samlet bidrag af mindst samme størrelsesorden **som den samlede EU-budgetfinansiering**. Dertil kommer evt. udgifter til **etablering og drift af** et nationalt koordinationscenter. Forslaget ventes at have positive erhvervsøkonomiske konsekvenser for danske virksomheder. Det kan ikke udelukkes, at forslaget vil have lovgivningsmæssige konsekvenser. Dette vil afhænge af det nationale koordinationscenters placering og kompetencer. Regeringen har fokus på cybersikkerhed og vil indgå i forhandlingerne om forslaget med henblik på at sikre, at et evt. europæisk kompetencecenter og tilhørende nationale netværk tilfører reel merværdi på omkostningseffektiv vis**, idet de statsfinansielle konsekvenser bør minimeres**.*

2. Baggrund

Kommissionen præsenterede 14. september 2017 sin meddelelse om cybersikkerhed, der udbygger og supplerer EU's cybersikkerhedsstrategi fra 2013. Meddelelsen indeholder en række elementer til styrkelse af cybersikkerheden i EU, herunder forslag om etablering af et europæisk cybersikkerhedskompetencecenter suppleret af et netværk af nationale koordinationscentre. Forslaget skal bl.a. ses som opfølgning på det offentligt-private partnerskab om cybersikkerhed etableret i 2016.

Rådet vedtog i november 2017 rådskonklusioner om cybersikkerhed og hilste i den forbindelse intentionen om et netværk af nationale koordinationscentre velkommen for at sikre innovation i den europæiske cybersikkerhedsindustri og udvikling af næste generation af teknologier, herunder AI,

quantum computing, blockchain og sikre digitale identiteter. Rådet noterede sig det planlagte europæiske cybersikkerhedsforskningscenter og understregede desuden, at netværket af kompetencecentre bør adressere et bredt spektrum af spørgsmål fra forskning til industripolitik.

Kommissionen har 6. juni 2018 fremlagt forslag til forordning om programmet for Det Digitale Europa for perioden 2021-2027 (KOM(2018)434). Et af programmets fem delområder vedrører cybersikkerhed og tillid. Delområdet skal styrke EU's industrielle potentiale og konkurrenceevne inden for cybersikkerhed og forbedre både den private og den offentlige sektors kapacitet til at beskytte europæiske borgere og virksomheder mod cybertrusler. Forordningen om oprettelse af et kompetencecenter for cybersikkerhed ***foreslås således*** finansiere***t*** delvist ***via programmet for*** Det Digitale Europa**.**

Midlerne ***afsat*** under delprogrammet ***forslås*** supplere***t af*** investeringer fra medlemsstaterne og vil blive brugt til at investere i avanceret cybersikkerhedsudstyr og -værktøjer samt relevant datainfrastruktur.

Det nuværende rammeprogram for forskning og innovation, Horisont 2020, indeholder et program for sikkerhedsforskning, herunder i cybersikkerhed. Kommissionen har 7. juni 2018 fremsat et forslag til rammeprogrammets efterfølger fra 2021 til 20***2***7, Horisont Europa (KOM(2018) 435 og KOM(2018) 436), herunder forslag om en fortsat indsats på cybersikkerhedsområdet. Der er ikke fremsat forslag til øremærket budget for indsatsen.

Kommissionens har ved KOM (2018) 630 af 12. september 2018 fremsat forslag til forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre. Forslaget er oversendt til Rådet 14. september 2018 i dansk sprogversion.

Kommissionen anfører, at forslaget har hjemmel i dels TEUF art. 188. stk. 1, hvorefter Rådet på forslag af Kommissionen og efter høring af Europa-Parlamentet og Det Økonomiske og Sociale Udvalg vedtager de i TEUF artikel 187 omhandlede bestemmelser om, at Unionen kan oprette fællesforetagender eller enhver anden struktur, der er nødvendig for korrekt gennemførelse af programmerne for forskning, teknologisk udvikling og demonstration i Unionen. Dels TEUF art. 173, stk. 3 om EU-industriens konkurrenceevne. Forslaget vil blive behandlet efter den almindelige lovgivningsprocedure.

3. Formål og Indhold

Kommissionens forslag indeholder forslag om 1) oprettelse af et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed 2) etablering af et netværk af nationale koordinationscentre på cybersikkerhedsområdet og 3) etablering af et cybersikkerhedskompetencefællesskab.

Oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed

Formålet med et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed er at bevare og udvikle teknologiske og industrielle kapaciteter vedrørende cybersikkerhed, øge konkurrenceevnen for cybersikkerhedsindustrien i EU og gøre cybersikkerhed til en konkurrencemæssig fordel for andre industrier i EU.

Samtidig vil kompetencecenteret ***skulle*** fungere som et fælles gennemførelsesorgan for forskellige EU-programmer i perioden 2021 til 2027 til støtte for cybersikkerhed (Det Digitale Europa og Horisont Europa) og øge synergierne mellem disse.

Kompetencecentret skal ***bl.a.***:

- fremme og koordinere arbejdet i de nationale koordinationscentres netværk og kompetencefællesskabet for cybersikkerhed
- bidrage til gennemførslen af cybersikkerhedsdelen af programmet for Det Digitale Europa og Horisont Europa-programmet ved at udmønte de afsatte midler gennem tilskud og indkøb
- forbedre de cybersikkerhedskapaciteter, viden og den infrastruktur, der står til rådighed for industrien, den offentlige sektor og forskningsverdenen
- ***bevare og udvikle de teknologiske og industrielle kapaciteter vedrørende cybersikkerhed***
- ***erhverve, opgradere, drive og stille cyberinfrastrukturer og -tjenester i forbindelse hermed til rådighed for erhvervslivet, herunder SMV'er, den offentlige sektor og forsknings- og videnskabskredse***
- bidrage til udbredelse af avancerede cybersikkerhedsprodukter og -løsninger
- forbedre forståelsen af internetsikkerhed og bidrage til at indhente kvalifikationsunderskuddet i EU vedrørende cybersikkerhed
- bidrage til at styrke forskning i og udvikling i EU af cybersikkerhed
- styrke samarbejdet mellem civilbeskyttelses- og forsvarsområdet mht. anvendelse af teknologier med dobbelt anvendelsesformål inden for cybersikkerhed

- styrke synergierne mellem civilbeskyttelses- og forsvarsdimensionerne af cybersikkerhed i forbindelse med Den Europæiske Forsvarsfond
- ***forvalte multinationale cyberforsvarsprojekter i regi af den Europæiske Forsvarsfond, når medlemsstaterne anmoder herom***
- ***kunne være ansvarligt for den overordnede gennemførelse af relevante fælles indkøb***.

Kompetencecentret skal samarbejde med EU's relevante institutioner, organer, kontorer og agenturer, herunder:

- ***Den Europæiske Unions Agentur for Net- og Informationssikkerhed***
- ***IT-Beredskabsenheden (CERT-EU)***
- ***Tjenesten for EU's Optræden Udadtil***
- ***Det Fælles Forskningscenter under Kommissionen***
- ***Forvaltningsorganet for Forskning***
- ***Forvaltningsorganet for Innovation og Netværk***
- ***Det Europæiske Center for Bekæmpelse af Cyberkriminalitet hos Europol***
- ***Det Europæiske Forsvarsagentur.***

Kompetencecentret ***skal*** bestå af en bestyrelse med en repræsentant for hver medlemsstat samt fem repræsentanter for Kommissionen, en administrerende direktør og et industrielt og videnskabeligt rådgivende organ. Bestyrelsen ***vil*** udgør***e*** det øverste beslutningsorgan, hvor kun medlemsstater, der deltager i finansieringen, har stemmeret.

Kompetencecenteret vil desuden ***skulle*** fremme forskning for at bidrage til standardiserings- og certificeringsprocesser. Det gælder særligt de, der vedrører cybersikkerhedscertificeringsordninger som defineret i forordningen om cybersikkerhed (KOM (2017) 477/final 3).

<u>Netværk af nationale koordinationscentre</u>

Kommissionen foreslår, at alle medlemsstater udpeger et nationalt koordinationscenter, der skal støtte det europæiske kompetencecenter med at udvikle teknologi og kapacitet på cybersikkerhedsområdet, der sikrer det digitale indre marked og øger konkurrenceevnen for EU's cybersikkerhedsindustri.

De nationale koordinationscentre skal udover den nødvendige administrative kapacitet have adgang til relevant teknologisk ekspertise på cybersikkerhedsområdet og kapacitet til at koordinere med industrien, den offentlige sektor og forskningsverdenen.

De nationale koordinationscentre skal:

- støtte det europæiske kompetencecenter med at opfylde dets mål
- lette industriens og andre aktørers deltagelse på medlemsstatsniveau i grænseoverskridende projekter
- sammen med kompetencecenteret bidrage til at identificere og møde sektorspecifikke industrielle udfordringer vedrørende cybersikkerhed
- fungere som kompetencenetværk for cybersikkerhed og kontaktpunkt for kompetencecentret
- tilstræbe at skabe synergivirkninger med relevante aktiviteter på nationalt og regionalt plan
- gennemføre specifikke aktioner, som kompetencecentret har ydet tilskud til, herunder ved ydelse af finansiel støtte til tredjeparter i overensstemmelse med artikel 204 i forordning ***2018/1046*** [ny finansforordning] på de betingelser, der er fastsat i de pågældende tilskudsaftaler
- fremme og formidle relevante resultater af arbejdet i netværket, kompetencefællesskabet for cybersikkerhed og kompetencecentret på nationalt eller regionalt niveau
- vurdere anmodninger fra enheder, der er etableret i samme medlemsstat som koordinationscentret, om at blive en del af kompetencefællesskabet for cybersikkerhed.

Kompetencefællesskabet for cybersikkerhed

Kompetencefællesskabet for cybersikkerhed skal bidrage til kompetencecentrets opgaver og styrke og formidle cybersikkerhedsekspertise i hele EU.

Kompetencefællesskabet for cybersikkerhed skal bestå af industrielle, akademiske og almennyttige forskningsorganisationer og sammenslutninger samt offentlige organer og andre enheder, der beskæftiger sig med operationelle og tekniske spørgsmål. Det skal samle de vigtigste aktører med hensyn til teknologisk og industriel kapacitet for cybersikkerhed i EU med relevant ekspertise på mindst et af følgende områder: (a) forskning, (b) industriel udvikling og (c) uddannelse.

Medlemmerne af kompetencefællesskabet for cybersikkerhed skal:

- støtte kompetencecentret i at udføre sine opgaver og med henblik herpå arbejde tæt sammen med kompetencecentret og de relevante nationale koordinationscentre
- deltage i aktiviteter, der fremmes af kompetencecentret og nationale koordinationscentre
- deltage i arbejdsgrupper nedsat af bestyrelsen for kompetencecentret med det formål at udføre særlige aktiviteter som fastsat af kompetencecentrets arbejdsplan

- støtte kompetencecentret og de nationale koordinationscentre med at fremme specifikke projekter
- fremme og formidle relevante resultater af de aktiviteter og projekter, der gennemføres i fællesskabet.

4. Europa Parlamentets udtalelser

Europa-Parlamentets udtalelser foreligger endnu ikke.

Forslaget vil blive behandlet i Europa-Parlamentets udvalg for Industri, Forskning og Energi (ITRE) og forventes sat til afstemning den 19. februar 2019.

5. Nærhedsprincippet

Kommissionen anfører, at omfanget og skalaen af de teknologiske udfordringer på cybersikkerhedsområdet og den utilstrækkelige koordination af indsatsen i og på tværs af industrien, den offentlige sektor og forskningsmiljøerne kræver, at EU yderligere støtter op og bl.a. sikrer bedre styring af viden og aktiver. Dette kræver ifølge Kommissionen ressourcer og ekspertise i et omfang, som de enkelte medlemsstater ikke besidder, hvorfor målene ikke kan opnås af medlemsstaterne selv.

Regeringen finder ikke anledning til at tilsidesætte Kommissionen vurdering af nærhedsprincippet.

6. Gældende dansk ret

Ikke relevant.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Det kan ikke udelukkes, at forslaget om et nationalt koordinationscenter vil have lovgivningsmæssige konsekvenser. Dette vil bl.a. afhænge af, hvilke opgaver et nationalt koordinationscenter vil skulle løse samt, om et sådant koordinationscenters opgaver kan løses inden for de eksisterende eller allerede planlagte strukturer eller vil kræve oprettelse af en ny enhed.

Økonomiske konsekvenser
Forslaget forventes at medføre væsentlige statsfinansielle konsekvenser, dels via EU's budget og dels via afledte nationale udgifter og et evt. medfinansieringsbidrag ved dansk deltagelse i samarbejdet.

Ifølge forslaget vil EU***-budgettet***s bidrag til kompetencecentret i perioden 2021-27 udgøre 1.981.668.000 euro (løbende priser) fra det af Kommissionen foreslåede program for Det Digitale Europa samt et endnu ikke fastsat beløb fra det af Kommissionen foreslåede program Horisont Europa. Forudsat en dansk finansieringsandel på ca. 2 pct. af EU's udgifter som i dag, vil Danmarks bidrag til EU-finansieringen gennem programmet for det digitale Europa svare til ca. 300 mio. kr. ***over perioden.*** Hertil kommer det endnu ikke fastsatte beløb finansieret via Horisont Europa-programmet.

Deltagende medlemsstater vil ***jf. forslaget*** herudover også skulle yde et samlet bidrag af mindst samme størrelsesorden som finansieret via EU-budgettet. For Danmark vil det betyde et forventet merbidrag på min. 300 mio. kr. ***over perioden*** samt et endnu ukendt beløb svarende til den danske finansieringsandel af bidraget fra Horisont Europa-programmet.

Herudover vil der kunne forventes statsfinansielle konsekvenser via afledte nationale udgifter til oprettelsen af et nationalt koordinationscenter, hvad enten dette sker som et nyt center eller i rammen af et eksisterende. Det vurderes endnu for tidligt at estimere omfanget heraf, idet de konkrete økonomiske konsekvenser vil blive analyseret nærmere. Det er endnu uklart om eller i hvilket omfang, omkostningerne til det nationale koordinationscenter ligger udover de midler, der allerede er afsat til udmøntning af regeringens nationale strategi for cyber- og informationssikkerhed. Det bemærkes, at de afledte nationale udgifter som udgangspunkt vil skulle afholdes inden for de berørte ministeriers eksisterende bevillingsrammer, jf. retningslinjerne for den danske EU-beslutningsprocedure og budgetvejledningens bestemmelser herom.

Forslaget vurderes at have positive erhvervsøkonomiske og samfundsøkonomiske konsekvenser, da det forventes at kunne komme danske virksomheder og myndigheder til gavn gennem øget beskyttelse samt en styrkelse af EU's industrielle potentiale og konkurrenceevne inden for cybersikkerhed.

8. Høring

Forslaget ***har været*** i høring i specialudvalget for Konkurrenceevne, vækst og forbrugerspørgsmål og specialudvalget for Forskning med frist ***for bemærkninger*** 25. oktober 2018. ***Der er modtaget høringssvar fra Finans Danmark.***

Finans Danmark hilser forslag til forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre velkomment. Finans Danmark støtter forslaget om at styrke den europæiske cybersikkerhedsindustris konkurrenceevne og finder, at dette kan medvirke til at forbedre cybersikkerheden i EU. Finans Danmark vurderer, at den øgede digitalisering og konstante udvikling i trusselsbilledet stiller større krav til den enkelte virksomheds færdigheder og viden om digital sikkerhed. De rette kompetencer er altafgørende, og cyberkompetencer er en mangelvare, både hvad angår generalister og specialister. Derfor finder Finans Danmark alle initiativer, der kan forbedre europæiske industri-, teknologi- og forskningskompetencer inden for cybersikkerhed, nødvendige og efterspurgte.

9. Generelle forventninger til andre landes holdninger

Medlemsstaterne udtrykker generelt støtte til forslagets overordnede formål, herunder især behovet for at fastholde og udvikle de nødvendige teknologiske og industrielle cybersikkerhedskapaciteter med henblik på at sikre udvikling af det Digitale Indre Marked og øge konkurrenceevnen for EU's cybersikkerhedsindustri samt øge koordinationen mellem EU's cybersikkerhedsforskningsprogrammer.

Medlemsstaterne har imidlertid generelt også et forbehold i forhold til, at programmerne for Det Digitale Europa og Horisont Europa, der skal bidrage med finansiering til forslaget, begge er under forhandling, og at resultatet derfor ikke kendes. Endvidere har medlemsstaterne efterspurgt større klarhed omkring afgrænsning og synergi i forhold til allerede eksisterende strukturer i EU.

Et antal medlemsstater efterspørger klarhed omkring metoden for beregning af medlemsstaternes finansielle bidrag, herunder at metoden bliver fastlagt i forbindelse med forhandling af forslaget og ikke overlades til kompetencecenterets bestyrelse.

Flere medlemsstater har endnu ikke en afstemt national position til forslaget.

10. Regeringens generelle holdning

Regeringen har generelt fokus på cybersikkerhed og vil indgå i forhandlingerne om forslaget med fokus på at sikre, at et europæisk kompetencecenter tilfører reel merværdi på en omkostningseffektiv vis, herunder understøtter udviklingen af et sikkert digitalt indre marked. Regeringen har desuden fokus på, at medlemsstaternes rolle og ansvar for egen cybersikkerhed og modsvar på cybertrusler fastholdes, og at omkostningerne forbundet med forslaget står mål med de forventede gevinster***, idet de statsfinansielle konsekvenser bør minimeres.***

Regeringen fremlagde i 2018 en national strategi for cyber- og informationssikkerhed. Strategien fokuserer på 1) at opruste i staten og samfundskritiske sektorer til at beskytte samfundsmæssige funktioner mod cyberangreb, 2) øge kompetenceniveau både i den brede befolkning og gennem forskning i ny teknologi samt videndeling og koordination i partnerskaber og 3) en fælles indsats med sektorvise delstrategier i samfundskritiske sektorer, styrket national koordination og internationalt engagement.

Kommissionens forslag til forordningen er overordnet i tråd med den danske strategi og oprustning på cybersikkerhedsområdet***, om end med et andet fokus, idet forordningsforslaget er mere erhvervsrettet og ikke målrettet kritiske sektorer***. Tiltagene i forordningen vurderes at kunne understøtte samarbejde, koordination, forebyggelse og videndeling i relation til cybersikkerhed på tværs af EU.

Regeringen vil arbejde for konsistens mellem forordningens initiativer og regeringens nationale strategi om cyber- og informationssikkerhed herunder særligt initiativerne rettet mod at skabe et højere kompetenceniveau. ***Der skal forsat arbejdes på at højne kompetenceniveauet for cybersikkerhed i de samfundskritiske sektorer, herunder i de statslige beredskaber.***

Regeringen støtter generelt arbejdet med at styrke EU's industrielle potentiale og konkurrenceevne inden for cybersikkerhed samt forbedre både den private og offentlige sektors kapaciteter på området som led i at øge tilliden til den digitale transformation.

Regeringen har endvidere fokus på at få afklaret kompetencecentrets ***intenderede*** rolle og funktion i praksis, herunder ikke mindst i lyset af de betydelige statsfinansielle implikationer forbundet med forslaget. I Horisont 2020 er den tilsvarende rolle tildelt programkomiteen for sikkerhedsprogrammet. Det er vigtigt, at der bliver etableret en transparent og effektiv struktur for denne opgavevaretagelse. Dette er også relevant i forhold til ***de forventede tiltag om at facilitere forskning og udvikling i forhold***

til den kommende ***Europæiske F***orsvarsfond, ***under hensyntagen til arbejdet med Forsvarsfonden generelt***.

Desuden er det vigtigt for regeringen, at drøftelser om forslaget ikke foregriber forhandlingerne om EU's kommende finansielle ramme for perioden 2021-2027, herunder sektorforslagene vedr. Horisont Europa og Det Digitale Europa.

Regeringen finder det vigtigt, at det bliver nemt for både virksomheder og offentlige myndigheder at anvende aktiviteter finansieret under det af Kommissionen foreslåede program Det Digitale Europa. Det er således vigtigt for regeringen, at administrationen ikke bliver for tung.

11. Tidligere forelæggelser for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg. Rådskonklusioner om cybersikkerhed blev forelagt Europaudvalget 17. november 2017. ***Grund- og nærhedsnotat er oversendt 15. oktober 2018.***

E