EUROPA-
KOMMISSIONEN

Strasbourg, den 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester

(EØS-relevant tekst)

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Denne begrundelse ledsager forslaget til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) 2019/881[1] for så vidt angår administrerede sikkerhedstjenester.

Dette forslag til en målrettet ændring har til formål at gøre det muligt ved hjælp af Kommissionens gennemførelsesretsakter at vedtage europæiske cybersikkerhedscertificeringsordninger for "administrerede sikkerhedstjenester" i lighed med informations- og teknologiprodukter, -tjenester og -processer, som allerede er omfattet af forordningen om cybersikkerhed. Administrerede sikkerhedstjenester spiller en stadig vigtigere rolle i forbindelse med forebyggelse og afbødning af cybersikkerhedshændelser.

I sine konklusioner af 23. maj 2022[2] om udviklingen af Den Europæiske Unions cyberposition opfordrede Rådet Unionen og medlemsstaterne til at styrke indsatsen for at øge det generelle cybersikkerhedsniveau, f.eks. ved at lette fremkomsten af udbydere af cybersikkerhedstjenester, man kan have tillid til, og understregede, at fremme af udviklingen af sådanne udbydere bør være en prioritet for EU's industripolitik på cybersikkerhedsområdet. Rådet opfordrede også Kommissionen til at fremsætte forslag om mulighederne for at fremme udviklingen af en pålidelig branche for cybersikkerhedstjenester. Certificering af administrerede sikkerhedstjenester er et effektivt middel til at sikre tillid til kvaliteten af disse tjenester og dermed lette etableringen af en pålidelig europæisk cybersikkerhedsindustri.

I den fælles meddelelse "EU's politik for cyberforsvar", som blev vedtaget af Kommissionen og den højtstående repræsentant den 10. november 2022[3], blev det meddelt, at Kommissionen vil undersøge udviklingen af cybersikkerhedscertificeringsordninger på EU-plan for cybersikkerhedsindustrien og private virksomheder. Udbydere af administrerede sikkerhedstjenester skal også spille en vigtig rolle i EU's cybersikkerhedsreserve, hvoraf den gradvise opbygning understøttes af cybersolidaritetsloven, der foreslås parallelt med denne forordning. EU's cybersikkerhedsreserve skal anvendes til at støtte foranstaltninger vedrørende indsats og omgående genopretning i tilfælde af væsentlige og omfattende cybersikkerhedshændelser. De relevante cybersikkerhedstjenester, der leveres af "betroede udbydere" som omhandlet i cybersolidaritetsloven, svarer til de "administrerede sikkerhedstjenester" i dette forslag.

Nogle medlemsstater er allerede begyndt at vedtage certificeringsordninger for administrerede sikkerhedstjenester. Der er derfor en stigende risiko for fragmentering af det indre marked for administrerede sikkerhedstjenester på grund af manglende overensstemmelse mellem de cybersikkerhedscertificeringsordninger, der indføres i Unionen. Dette forslag gør det muligt at etablere europæiske cybersikkerhedscertificeringsordninger for de omhandlede tjenester for at forhindre en sådan fragmentering.

---

[1] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) EUT L 151/15 af 7.6.2019.

[2] 9364/22.

[3] JOIN(2022) 49 final.

- **Sammenhæng med de gældende regler på samme område**

Dette forslag er i overensstemmelse med forordningen om cybersikkerhed, som det indebærer ændringer af. Det bygger på bestemmelserne i nævnte forordning, der tilpasses, så de også omfatter administrerede sikkerhedstjenester. De foreslåede ændringer er begrænset til det strengt nødvendige og ændrer ikke forordningens karakteristika eller funktion.

Dette forslag er også i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet)[4]. Udbydere af administrerede sikkerhedstjenester anses for at være væsentlige eller vigtige enheder, der tilhører en sektor af særlig kritisk betydning i henhold til direktiv (EU) 2022/2555. Det fremgår af direktivets betragtning 86, at udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand spiller en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser. Udbydere af administrerede sikkerhedstjenester har imidlertid også selv været mål for cyberangreb og udgør en særlig risiko på grund af deres tætte integration i kundernes aktiviteter. Væsentlige og vigtige enheder i henhold til direktiv (EU) 2022/2555 bør derfor udvise forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.

Dette forslag har til formål at forbedre kvaliteten af de administrerede sikkerhedstjenester og gøre dem mere sammenlignelige. Forslaget gør det dermed muligt for væsentlige og vigtige enheder at udvise øget omhu i forbindelse med udvælgelsen af en udbyder af administrerede sikkerhedstjenester som krævet i henhold til direktiv (EU) 2022/2555. Desuden er definitionen af "administrerede sikkerhedstjenester" i dette forslag afledt af og ligger tæt op ad definitionen af "udbydere af administrerede sikkerhedstjenester" i direktiv (EU) 2022/2555. Forslaget supplerer derfor i høj grad NIS 2-direktivet.

Endelig supplerer dette forslag den foreslåede cybersolidaritetslov. Den foreslåede cybersolidaritetslov indeholder bestemmelser om en proces til udvælgelse af udbydere til en cybersikkerhedsreserve på EU-plan, hvori der bl.a. bør tages hensyn til, om disse udbydere har en europæisk eller national cybersikkerhedscertificering. Fremtidige certificeringsordninger for administrerede sikkerhedstjenester vil således spille en væsentlig rolle for gennemførelsen af cybersolidaritetsloven.

- **Sammenhæng med Unionens politik på andre områder**

Dette forslag berører ikke overensstemmelsen mellem forordningen om cybersikkerhed og forordning (EU) 2016/679 (den generelle forordning om databeskyttelse, "GDPR")[5] og dens bestemmelser om indførelse af certificeringsmekanismer og databeskyttelsesmærkninger og -mærker med henblik på at påvise dataansvarliges og databehandleres overholdelse af denne forordning. Forordningen om cybersikkerhed berører ikke certificeringen af databehandlingsoperationer, herunder hvis sådanne operationer er indeholdt i produkter og tjenester, som foretages i henhold til den generelle forordning om databeskyttelse.

Desuden berører dette forslag ikke cybersikkerhedsforordningens forenelighed med forordning (EF) nr. 765/2008 om akkrediterings- og markedstilsynskrav[6], navnlig for så vidt

4 EUT L 333 af 27.12.2022 s. 810.
5 EUT L 119/1 af 4.5.2016.
6 EUT L 218/30 af 13.8.2008.

angår rammen for nationale akkrediteringsorganer og overensstemmelsesvurderingsorganer og nationale certificeringstilsynsmyndigheder.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Dette forslag ændrer forordningen om cybersikkerhed, hvis retsgrundlag er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Som det er tilfældet med forordningen om cybersikkerhed, har dette forslag til formål at undgå fragmentering af det indre marked, navnlig ved at gøre det muligt at vedtage europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester. Medlemsstaterne er begyndt at vedtage certificeringsordninger for administrerede sikkerhedstjenester. Der er således en konkret risiko for fragmentering af det indre marked for disse tjenesteydelser, som nærværende forslag har til formål at afhjælpe. Derfor er artikel 114 i TEUF det relevante retsgrundlag for dette initiativ.

- **Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)**

Målsætningen om at gøre det muligt at vedtage europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester og undgå fragmentering af det indre marked kan ikke opfyldes på nationalt plan, men kun på EU-plan. Desuden tilbydes administrerede sikkerhedstjenester, som er genstand for den foreslåede ændring, af udbydere, der er aktive i hele Unionen, og det samme gælder deres største potentielle kunder. En indsats på EU-plan er derfor både nødvendig og mere effektiv end en indsats på nationalt plan.

- **Proportionalitetsprincippet**

Forslaget er en målrettet ændring af forordningen om cybersikkerhed. Det er begrænset til det strengt nødvendige for at opfylde målsætningen, nemlig at gøre det muligt at vedtage europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester i lighed med IKT-produkter, IKT-tjenester og IKT-processer. De foreslåede ændringer indebærer navnlig en tilpasning af anvendelsesområdet for den europæiske ramme for cybersikkerhedscertificering, så den nu omfatter "administrerede sikkerhedstjenester", der indføres en definition af disse tjenester i overensstemmelse med NIS 2-direktivet, og sikkerhedsmålsætningerne for den europæiske cybersikkerhedscertificering ændres for at tilpasse den til "administrerede sikkerhedstjenester". De øvrige ændringer er af teknisk art og har til formål at sikre, at de relevante artikler også finder anvendelse på "administrerede sikkerhedstjenester". Det foreslåede initiativ står således i et rimeligt forhold til målsætningen.

- **Valg af retsakt**

Da forslaget ændrer forordning (EU) 2019/881, er den relevante retsakt en forordning.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSENTER OG KONSEKVENSANALYSER

- **Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning**

Ikke relevant.

- **Høringer af interessenter**

Der er gennemført målrettede høringer af medlemsstaterne og ENISA. Under disse høringer beskrev medlemsstaterne deres nuværende aktiviteter og synspunkter med hensyn til certificering af administrerede sikkerhedstjenester. ENISA redegjorde for sine synspunkter og resultaterne af drøftelserne med medlemsstaterne og interessenterne. De bemærkninger og oplysninger, der er modtaget fra medlemsstaterne og ENISA, er inddraget i dette forslag.

- **Indhentning og brug af ekspertbistand**

Ikke relevant.

- **Konsekvensanalyse**

Der er anmodet om en undtagelse fra kravet om en konsekvensanalyse, da forslaget er en meget begrænset og målrettet ændring af forordningen om cybersikkerhed. Det vil give Kommissionen mulighed for ved gennemførelsesretsakter at vedtage certificeringsordninger for "administrerede sikkerhedstjenester" i lighed med IKT-produkter, IKT-tjenester og IKT-processer, som allerede er omfattet af forordningen. Ændringen vil imidlertid først få virkning, når sådanne certificeringsordninger vedtages på et senere tidspunkt. Desuden vil ændringen ikke ændre certificeringsordningernes frivillige karakter.

- **Målrettet regulering og forenkling**

Ikke relevant.

- **Grundlæggende rettigheder**

Forslaget har ingen forudsigelige konsekvenser for beskyttelsen af de grundlæggende rettigheder.

4. VIRKNINGER FOR BUDGETTET

Ingen.

5. ANDRE FORHOLD

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

De bestemmelser, der skal ændres ved forslaget, bliver evalueret som led i den periodiske evaluering af forordningen om cybersikkerhed, der skal foretages af Kommissionen i overensstemmelse med artikel 67 heri. Ved den evaluering vurderer Kommissionen bl.a. virkningen og effektiviteten af bestemmelserne vedrørende rammerne for cybersikkerhedscertificering med hensyn til målsætningerne om at sikre et tilstrækkeligt niveau for IKT-produkters, IKT-tjenesters og IKT-processers cybersikkerhed i Unionen og forbedre det indre markeds funktion. Forslaget indeholder en ændring, der sikrer, at evalueringen også omfatter administrerede sikkerhedstjenester. Kommissionen sender også en rapport om evalueringen og konklusionerne heraf til Europa-Parlamentet, Rådet og ENISAs bestyrelse og offentliggør resultaterne af rapporten.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Forslaget indeholder to artikler. Artikel 1 indeholder ændringerne af forordning (EU) 2019/881, og artikel 2 vedrører ikrafttrædelsen. Artikel 1 indeholder målrettede ændringer af

anvendelsesområdet for den europæiske ramme for cybersikkerhedscertificering i forordningen om cybersikkerhed, så rammen herefter omfatter "administrerede sikkerhedstjenester" (artikel 1 og 46 i forordningen om cybersikkerhed). Forslaget fastsætter en definition af disse tjenester, som er nøje afstemt efter definitionen af "udbydere af administrerede sikkerhedstjenester" i NIS 2-direktivet (artikel 2 i forordningen om cybersikkerhed). Forslaget tilføjer også en ny artikel 51a om sikkerhedsmålsætningerne for europæisk cybersikkerhedscertificering, hvor målsætningerne er tilpasset "administrerede sikkerhedstjenester". Endelig indeholder forslaget en række tekniske ændringer for at sikre, at de relevante artikler også finder anvendelse på "administrerede sikkerhedstjenester".

2023/0108 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg,

under henvisning til udtalelse fra Regionsudvalget,

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets forordning (EU) 2019/881[7] fastsætter en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, IKT-tjenester og IKT-processer i Unionen samt at undgå fragmentering af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i Unionen.

(2) Administrerede sikkerhedstjenester, som er tjenester, der består i at udføre eller yde bistand til aktiviteter vedrørende kundernes risikostyring i forbindelse med cybersikkerhed, har fået stadig større betydning i forbindelse med forebyggelse og afbødning af cybersikkerhedshændelser. Udbydere af disse tjenester anses derfor for at være væsentlige eller vigtige enheder, der tilhører en sektor af særlig kritisk betydning i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[8]. Det fremgår af direktivets betragtning 86, at udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand spiller en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser. Udbydere af administrerede sikkerhedstjenester har imidlertid også selv været mål for

[7] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

[8] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

cyberangreb og udgør en særlig risiko på grund af deres tætte integration i kundernes aktiviteter. Væsentlige og vigtige enheder i henhold til direktiv (EU) 2022/2555 bør derfor udvise forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.

(3) Udbydere af administrerede sikkerhedstjenester spiller også en vigtig rolle i EU's cybersikkerhedsreserve, hvis gradvise etablering støttes af forordning (EU) .../.... [om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser]. EU's cybersikkerhedsreserve skal støtte indsatsen og tiltag til omgående genopretning i tilfælde af væsentlige og omfattende cybersikkerhedshændelser. Forordning (EU) .../... [om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser] fastsætter en udvælgelsesproces for de udbydere, der udgør EU's cybersikkerhedsreserve, som bl.a. bør tage hensyn til, om den pågældende udbyder har opnået en europæisk eller national cybersikkerhedscertificering. De relevante tjenester, der leveres af "betroede udbydere" i henhold til forordning (EU) .../... [om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser] svarer til "administrerede sikkerhedstjenester" i overensstemmelse med denne forordning.

(4) Certificering af administrerede sikkerhedstjenester er ikke kun relevant for udvælgelsesprocessen til EU's cybersikkerhedsreserve, men også en vigtig kvalitetsindikator for private og offentlige enheder, der har til hensigt at købe sådanne tjenester. På grund af de administrerede sikkerhedstjenesters kritiske karakter og følsomheden af de data, der behandles, kan certificeringen tjene som vigtig vejledning og sikkerhed for mulige kunder med hensyn til tjenesternes pålidelighed. Europæiske certificeringsordninger for administrerede sikkerhedstjenester bidrager til at undgå fragmentering af det indre marked. Denne forordning har derfor til formål at forbedre det indre markeds funktion.

(5) Ud over udbredelsen af IKT-produkter, IKT-tjenester eller IKT-processer leverer administrerede sikkerhedstjenester ofte yderligere servicefunktioner, der afhænger af personalets kompetencer, ekspertise og erfaring. Et meget højt niveau af kompetencer, ekspertise og erfaring samt passende interne procedurer bør indgå i sikkerhedsmålsætningerne for at sikre en meget høj kvalitet i de administrerede sikkerhedstjenester, der leveres. For at sikre, at alle aspekter af en administreret sikkerhedstjeneste kan dækkes af en certificeringsordning, er det derfor nødvendigt at ændre forordning (EU) 2019/881.

Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 og afgav udtalelse den [DD/MM/ÅÅÅÅ] —

VEDTAGET DENNE FORORDNING:

Artikel 1

Ændringer af forordning (EU) 2019/881

I forordning (EU) 2019/881 foretages følgende ændringer:

1) Artikel 1, stk. 1, første afsnit, litra b), affattes således:

"b) en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, IKT-tjenester og IKT-processer samt administrerede sikkerhedstjenester i Unionen, samt at undgå fragmentering af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i Unionen."

2) Artikel 2 ændres således:

a) Nr. 9, 10 og 11 affattes således:

"9) "europæisk cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er fastsat på EU-plan, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af specifikke IKT-produkter, IKT-tjenester og IKT-processer eller administrerede sikkerhedstjenester

"10) "national cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er udviklet og vedtaget af en national offentlig myndighed, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af IKT-produkter, IKT-tjenester og IKT-processer samt administrerede sikkerhedstjenester, der er omfattet af den pågældende ordning

11) "europæisk cybersikkerhedsattest": et dokument udstedt af et relevant organ, som attesterer, at et givet IKT-produkt, en given IKT-tjeneste eller en given IKT-proces eller en administreret sikkerhedstjeneste er blevet evalueret med henblik på overensstemmelse med specifikke sikkerhedskrav fastsat i en europæisk cybersikkerhedscertificeringsordning

b) Følgende nummer indsættes:

"14a) "administreret sikkerhedstjeneste": en tjeneste, der består i at udføre aktiviteter vedrørende styring af cybersikkerhedsrisici eller yde bistand til sådanne aktiviteter, herunder reaktion på hændelser, penetrationstest, sikkerhedsrevisioner og konsulentbistand"

c) Nr. 20), 21) og 22) affattes således:

"20) "*tekniske specifikationer*": et dokument, der fastsætter de tekniske krav, som et IKT-produkt, en IKT-tjeneste, en IKT-proces eller en *administreret sikkerhedstjeneste* skal opfylde eller de dertil hørende overensstemmelsesvurderingsprocedurer

21) "tillidsniveau": et grundlag for tillid til, at et IKT-produkt, en IKT-tjeneste, en IKT-proces eller en administreret sikkerhedstjeneste opfylder sikkerhedskravene i en bestemt europæisk cybersikkerhedscertificeringsordning, og en angivelse af, på hvilket niveau et IKT-produkt, en IKT-tjeneste, en IKT-proces eller en administreret sikkerhedstjeneste er blevet evalueret uden som sådan at måle IKT-produktets, IKT-tjenestens, IKT-processens eller den administrerede sikkerhedstjenestes sikkerhed

22) "selvvurdering af overensstemmelse": en handling foretaget af en producent eller udbyder af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, der evaluerer, hvorvidt IKT-produkterne,

IKT-tjenesterne, IKT-processerne eller de administrerede sikkerhedstjenester opfylder kravene i en specifik europæisk cybersikkerhedscertificeringsordning"

3) Artikel 4, stk. 6, affattes således

"6. ENISA fremmer brugen af europæisk cybersikkerhedscertificering med henblik på at undgå fragmentering af det indre marked. ENISA bidrager til etablering og vedligeholdelse af en europæisk ramme for cybersikkerhedscertificering, jf. afsnit III, for at øge gennemsigtigheden af IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters cybersikkerhedsniveau og dermed styrke tilliden til det digitale indre marked og dets konkurrenceevne."

4) Artikel 8 ændres således:

a) Stk. 1 affattes således:

"1. ENISA støtter og fremmer udviklingen og gennemførelsen af Unionens politik vedrørende cybersikkerhedscertificering af IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester som fastsat i denne forordnings afsnit III ved:

a) løbende at overvåge udviklingen på beslægtede standardiseringsområder og anbefale passende tekniske specifikationer til brug for udvikling af europæiske cybersikkerhedscertificeringsordninger i henhold til artikel 54, stk. 1, litra c), i tilfælde, hvor der ikke findes standarder

b) forberede forslag til europæiske cybersikkerhedscertificeringsordninger ("forslag til ordninger") for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester i overensstemmelse med artikel 49

c) evaluere vedtagne europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med artikel 49, stk. 8

d) deltage i peerreviews i henhold til artikel 59, stk. 4

e) bistå Kommissionen med at varetage sekretariatsfunktionen for ECCG i henhold til artikel 62, stk. 5."

b) Stk. 3 affattes således:

"3. ENISA samler og offentliggør retningslinjer og udvikler god praksis vedrørende cybersikkerhedskrav til IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester i samarbejde med nationale cybersikkerhedscertificeringsmyndigheder og branchen på en formaliseret, struktureret og gennemsigtig måde."

c) Stk. 5 affattes således:

"5. ENISA fremmer indførelse og udbredelse af europæiske og internationale standarder for risikostyring og for IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters sikkerhed."

5) Artikel 46, stk. 1 og 2, affattes således:

"1. Den europæiske ramme for cybersikkerhedscertificering etableres for at forbedre betingelserne for det indre markeds funktion ved at øge

cybersikkerhedsniveauet i Unionen og muliggøre en harmoniseret tilgang på EU-plan til europæiske cybersikkerhedscertificeringsordninger for at skabe et digitalt indre marked for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester."

2. Den europæiske ramme for cybersikkerhedscertificering definerer en mekanisme til fastlæggelse af europæiske cybersikkerhedscertificeringsordninger. Mekanismen tjener til attestering af, at IKT-produkter, IKT-tjenester og IKT-processer, der er evalueret i overensstemmelse med sådanne ordninger, opfylder de fastlagte sikkerhedskrav med henblik på at beskytte tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data, der lagres, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, tjenester og processer, i hele deres livscyklus. Derudover tjener mekanismen til at attestere, at administrerede sikkerhedstjenester, der er evalueret i overensstemmelse med sådanne ordninger, opfylder de fastlagte sikkerhedskrav med henblik på at beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der tilgås, behandles, lagres eller overføres i forbindelse med leveringen af disse tjenester, og at disse tjenester løbende leveres med den nødvendige kompetence, ekspertise og erfaring af personale med et meget højt niveau af relevant teknisk viden og faglig integritet."

6) Artikel 47, stk. 2 og 3, affattes således:

"2. Unionens rullende arbejdsprogram skal navnlig omfatte en liste over IKT-produkter, IKT-tjenester og IKT-processer eller kategorier heraf og administrerede sikkerhedstjenester, der vil kunne drage fordel af at være omfattet af en europæisk cybersikkerhedscertificeringsordning.

3. Tilføjelse af bestemte IKT-produkter, IKT-tjenester, IKT-processer eller kategorier heraf eller af administrerede sikkerhedstjenester i Unionens rullende arbejdsprogram skal være begrundet med et eller flere af følgende forhold:

a) tilgængeligheden og udviklingen af nationale cybersikkerhedscertificeringsordninger, der omfatter en bestemt kategori af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, og navnlig for så vidt angår risikoen for fragmentering

b) relevant EU- eller national ret eller politik

c) efterspørgslen på markedet

d) udviklingen i cybertrusselsbilledet

e) anmodning om udarbejdelse af et specifikt forslag til ordning fra ECCG."

7) Artikel 49, stk. 7, affattes således:

"7. Kommissionen kan på grundlag af det af ENISA udarbejdede forslag til ordning vedtage gennemførelsesretsakter vedrørende europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der opfylder kravene i artikel

51, 52 og 54. Gennemførelsesretsakterne vedtages efter undersøgelsesproceduren i artikel 66, stk. 2.".

8) Artikel 51 ændres således:

a) Overskriften affattes således:

Sikkerhedsmålsætninger for europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, IKT-tjenester og IKT-processer

b) Indledningen affattes således:

"En europæisk cybersikkerhedscertificeringsordning for IKT-produkter, IKT-tjenester eller IKT-processer skal være udformet til, alt efter relevans, som minimum at opfylde følgende sikkerhedsmålsætninger:"

9) Følgende artikel indsættes:

"Artikel 51a

Sikkerhedsmålsætninger for europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester

"En europæisk cybersikkerhedscertificeringsordning for administrerede sikkerhedstjenester skal være udformet til, alt efter relevans, som minimum at opfylde følgende sikkerhedsmålsætninger:

a) sikre, at de administrerede sikkerhedstjenester har den nødvendige kompetence, ekspertise og erfaring, herunder at det personale, der er ansvarligt for at levere disse tjenester, har et meget højt niveau af teknisk viden og kompetence på det specifikke område, tilstrækkelig og relevant erfaring og den højeste grad af faglig integritet

b) sikre, at udbyderen har indført passende interne procedurer til at sikre, at de administrerede sikkerhedstjenester til enhver tid leveres på et meget højt kvalitetsniveau

c) beskytte data, der tilgås, lagres, overføres eller på anden måde behandles i forbindelse med levering af administrerede sikkerhedstjenester, mod utilsigtet eller uautoriseret adgang, lagring, offentliggørelse, ødelæggelse, anden behandling, tab eller ændring eller manglende tilgængelighed

d) sikre hurtig genetablering af tilgængelighed af og adgang til data, tjenester og funktioner i tilfælde af en fysisk eller teknisk hændelse

e) sikre, at autoriserede personer, programmer eller maskiner udelukkende kan tilgå de data, tjenester eller funktioner, som de har adgangsret til

f) registrere og muliggøre vurdering af, hvilke data, tjenester og funktioner der er tilgået, anvendt eller på anden måde behandlet, på hvilket tidspunkt og af hvem

g) sikre, at de IKT-produkter, IKT-tjenester og IKT-processer [og hardware], der anvendes til levering af administrerede sikkerhedstjenester, er sikre som følge af standardindstillinger og indbygget sikkerhed, ikke har kendte sårbarheder og omfatter de seneste sikkerhedsopdateringer."

10) Artikel 52 ændres således:

a) Stk. 1 affattes således:

"1. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester: "grundlæggende", "betydeligt" eller "højt". Tillidsniveauet skal afspejle det risikoniveau, der er forbundet med den tilsigtede anvendelse af IKT-produktet, IKT-tjenesten, IKT-processen eller den administrerede sikkerhedstjeneste, hvad angår sandsynligheden for og virkningen af en hændelse."

b) Stk. 3 affattes således:

"3. De sikkerhedskrav, som svarer til tillidsniveauet, skal fremgå af den relevante europæiske cybersikkerhedscertificeringsordning, herunder de tilsvarende sikkerhedsfunktioner og den tilsvarende grad af stringens og dybde i den evaluering, som IKT-produktet, IKT-tjenesten, IKT-processen eller den administrerede sikkerhedstjeneste skal undergå."

c) Stk. 5, 6 og 7 affattes således:

"5. En europæisk cybersikkerhedsattest eller EU-overensstemmelseserklæring, der henviser til tillidsniveauet "grundlæggende", skal give sikkerhed for, at de IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som attesten eller EU-overensstemmelseserklæringen er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere de kendte grundlæggende risici for hændelser og cyberangreb. Evalueringsaktiviteterne skal som minimum omfatte en gennemgang af den tekniske dokumentation. Hvis en sådan gennemgang ikke er hensigtsmæssig, anvendes andre evalueringsaktiviteter med tilsvarende virkning.

6. En europæisk cybersikkerhedsattest, der henviser til tillidsniveauet "betydeligt", skal give sikkerhed for, at de IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som attesten er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere kendte cybersikkerhedsrisici og risikoen for hændelser og cyberangreb udført af aktører med begrænsede færdigheder og ressourcer. Evalueringsaktiviteterne, der gennemføres, skal som minimum omfatte følgende: en gennemgang med henblik på at påvise, at der ikke er offentligt kendte sårbarheder, og test for at påvise, at IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester udfører de nødvendige sikkerhedsfunktioner korrekt. Hvis

sådanne evalueringsaktiviteter ikke er hensigtsmæssige, anvendes andre evalueringsaktiviteter med tilsvarende virkning.

7. En europæisk cybersikkerhedsattest, der henviser til tillidsniveauet "højt", skal give sikkerhed for, at de IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som attesten er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere risikoen for avancerede cyberangreb udført af aktører med betydelige færdigheder og ressourcer. Evalueringsaktiviteterne, der gennemføres, skal som minimum omfatte følgende: en gennemgang med henblik på at påvise, at der ikke er offentligt kendte sårbarheder, test for at påvise, at IKT-produkterne, IKT-tjenesterne, IKT-processerne eller de administrerede sikkerhedstjenester på korrekt vis udfører de nødvendige sikkerhedsfunktioner på avanceret niveau, samt en vurdering af deres modstandsdygtighed over for drevne angribere ved hjælp af penetrationstest. Hvis sådanne evalueringsaktiviteter ikke er hensigtsmæssige, anvendes andre aktiviteter med tilsvarende virkning."

11) Artikel 53, stk. 1, 2 og 3, affattes således:

"1. En europæisk cybersikkerhedscertificeringsordning kan tillade, at der foretages selvvurdering af overensstemmelse, som producenter eller udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester har det fulde ansvar for. Selvvurdering af overensstemmelse er kun tilladt i forbindelse med IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester med lav risiko svarende til tillidsniveauet "grundlæggende".

2. Producenter og udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester kan udstede en EU-overensstemmelseserklæring, hvoraf det fremgår, at det er blevet påvist, at de krav, som er fastsat i ordningen, er opfyldt. Ved at udstede en sådan erklæring står producenter og udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester inde for, at IKT-produktet, IKT-tjenesten, IKT-processen eller den administrerede sikkerhedstjeneste stemmer overens med den pågældende ordnings krav.

3. Producenter og udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester stiller EU-overensstemmelseserklæringen, den tekniske dokumentation og alle øvrige relevante oplysninger vedrørende IKT-produkternes, IKT-tjenesternes eller de administrerede sikkerhedstjenesters overensstemmelse med ordningen til rådighed for den nationale cybersikkerhedscertificeringsmyndighed som omhandlet i artikel 58 i den periode, der er fastsat i den tilsvarende europæiske cybersikkerhedscertificeringsordning. En kopi af EU-overensstemmelseserklæringen indgives til den nationale cybersikkerhedscertificeringsmyndighed og til ENISA."

12) I artikel 54, stk. 1, foretages følgende ændringer:

a) Litra a) affattes således:

"a) certificeringsordningens genstand og omfang, herunder omfattede typer eller kategorier af IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester"

b) Litra j) affattes således:

"j) regler for overvågning af IKT-produkters, IKT-tjenesters-, IKT-processers og administrerede sikkerhedstjenesters overensstemmelse med de europæiske cybersikkerhedsattesters eller EU-overensstemmelseserklæringernes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav"

c) Litra l) affattes således:

"l) regler om følgerne for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som er blevet certificeret, eller for hvilke en EU-overensstemmelseserklæring er udstedt, men som ikke overholder kravene i ordningen"

d) Litra o) affattes således:

"o) angivelse af nationale eller internationale cybersikkerhedscertificeringsordninger, som dækker samme type eller kategorier af IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, sikkerhedskrav, evalueringskriterier og -metoder samt tillidsniveauer"

e) Litra q) affattes således:

"q) tilgængelighedsperioden af den EU-overensstemmelseserklæring, den tekniske dokumentation og alle de øvrige relevante oplysninger, der skal stilles til rådighed af producenter eller udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester"

13) Artikel 56 ændres således:

a) Stk. 1 affattes således:

"1. IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 49, formodes at overholde kravene i en sådan ordning."

b) Stk. 3 ændres således:

i) Første afsnit affattes således:

"Kommissionen vurderer regelmæssigt effektiviteten og anvendelsen af de vedtagne europæiske cybersikkerhedscertificeringsordninger, og hvorvidt en bestemt europæisk cybersikkerhedscertificeringsordning skal gøres obligatoriske ved hjælp af relevant EU-ret for at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, IKT-tjenester,

IKT-processer og administrerede sikkerhedstjenester i Unionen og forbedre det indre markeds funktion. Den første sådanne vurdering skal foretages senest den 31. december 2023 og efterfølgende vurderinger mindst hvert andet år derefter. Kommissionen identificerer på grundlag af resultatet af disse vurderinger de IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der er omfattet af en eksisterende certificeringsordning, og som skal omfattes af en obligatorisk certificeringsordning."

ii) I tredje afsnit foretages følgende ændringer:

(aa) Litra a) affattes således:

"a) tage hensyn til foranstaltningernes indvirkning på producenter og udbydere af sådanne IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester og på brugerne i form af omkostninger ved disse foranstaltninger samt de samfundsmæssige eller økonomiske fordele som følge af det forventede øgede sikkerhedsniveau for de pågældende IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester"

bb) Litra d) affattes således:

"d) tage hensyn til eventuelle gennemførelsesfrister og overgangsforanstaltninger eller -perioder under hensyntagen til navnlig foranstaltningens mulige indvirkning på producenter eller udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, herunder SMV'er"

c) Stk. 7 og 8 affattes således:

"7. Den fysiske eller juridiske person, der indgiver IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester til certificering, stiller alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, til rådighed for den i artikel 58 omhandlede nationale cybersikkerhedscertificeringsmyndighed, hvis denne myndighed er det organ, der udsteder den europæiske cybersikkerhedsattest, eller for det i artikel 60 omhandlede overensstemmelsesvurderingsorgan.

8. Indehaveren af en europæisk cybersikkerhedsattest underretter den myndighed eller det organ, der er omhandlet i stk. 7, om eventuelle efterfølgende opdagede sårbarheder eller uregelmæssigheder i forbindelse med de certificerede IKT-produkters, IKT-tjenesters, IKT-processers eller administrerede sikkerhedstjenesters sikkerhed, som kan have en indvirkning på overholdelsen af de med certificeringen forbundne krav. Vedkommende organ eller myndighed sender hurtigst muligt disse oplysninger til den pågældende nationale cybersikkerhedscertificeringsmyndighed."

14) Artikel 57, stk. 1 og 2, affattes således:

"1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, ophører med at have virkning fra det

tidspunkt, der fastsættes i den gennemførelsesretsakt, som vedtages i medfør af artikel 49, stk. 7, uden at dette dog berører nærværende artikels stk. 3. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, består fortsat.

2. Medlemsstaterne må ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som allerede er omfattet af en gældende europæisk cybersikkerhedscertificeringsordning."

15) Artikel 58 ændres således:

a) Stk. 7 ændres således:

i) Litra a) og b) affattes således:

"a) føre tilsyn med og håndhæve regler, der indgår i de europæiske cybersikkerhedscertificeringsordninger i henhold til artikel 54, stk. 1, litra j), til overvågning af, at IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester opfylder kravene i de europæiske cybersikkerhedsattester, der er udstedt på deres respektive område, i samarbejde med andre relevante markedsovervågningsmyndigheder

b) overvåge og håndhæve de forpligtelser, som påhviler producenter eller udbydere af IKT-produkter, IKT-tjenester IKT-processer eller administrerede sikkerhedstjenester, der er etableret på deres respektive område, og som foretager selvvurdering af overensstemmelse, navnlig forpligtelserne fastsat i artikel 53, stk. 2 og 3, og i den tilsvarende europæiske cybersikkerhedscertificeringsordning"

ii) Litra h) affattes således:

"h) samarbejde med andre nationale cybersikkerhedscertificeringsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters manglende overholdelse af denne forordnings eller specifikke europæiske cybersikkerhedscertificeringsordningers krav og"

b) Stk. 9 affattes således:

"9. De nationale cybersikkerhedscertificeringsmyndigheder skal samarbejde med hinanden og Kommissionen ved navnlig at udveksle oplysninger, erfaringer og god praksis med hensyn til cybersikkerhedscertificering og tekniske spørgsmål vedrørende IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters cybersikkerhed."

16) Artikel 59, stk. 3, litra b) og c), affattes således:

"b) procedurerne for tilsyn med og håndhævelse af reglerne for overvågning af, at IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester overholder europæiske cybersikkerhedsattester i henhold til artikel 58, stk. 7, litra a)

c) procedurerne for overvågning og håndhævelse af forpligtelserne for producenter eller udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester i henhold til artikel 58, stk. 7, litra b)"

17) Artikel 67, stk. 2 og 3, affattes således:

"2. Evalueringen skal også vurdere virkningen og effektiviteten af bestemmelserne i afsnit III i denne forordning med hensyn til målsætningerne om at sikre et tilstrækkeligt niveau for IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters cybersikkerhed i Unionen og forbedre det indre markeds funktion.

3. I evalueringen skal det også vurderes, om væsentlige cybersikkerhedskrav for adgang til det indre marked er nødvendige for at undgå, at IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der ikke opfylder grundlæggende cybersikkerhedskrav, kommer ind på EU-markedet."

Artikel 2

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i enhver medlemsstat.

Udfærdiget i Strasbourg, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*