Europa-Parlamentet
2019-2024

Mødedokument

A9-0307/2023

26.10.2023

***I
BETÆNKNING

om forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Udvalget om Industri, Forskning og Energi

Ordfører: Josianne Cutajar

Tegnforklaring

*	Høringsprocedure
***	Godkendelsesprocedure
***I	Almindelig lovgivningsprocedure (førstebehandling)
***II	Almindelig lovgivningsprocedure (andenbehandling)
***III	Almindelig lovgivningsprocedure (tredjebehandling)

(Proceduren afhænger af, hvilket retsgrundlag der er valgt i udkastet til retsakt)

Ændringsforslag til et udkast til retsakt

Ændringsforslag fra Parlamentet opstillet i to kolonner

Tekst, der udgår, er markeret med ***fede typer og kursiv*** i venstre kolonne.
Tekst, der udskiftes, er markeret med ***fede typer og kursiv*** i begge kolonner.
Ny tekst er markeret med ***fede typer og kursiv*** i højre kolonne.

Den første og den anden linje i informationsblokken til hvert ændringsforslag angiver den relevante passage i det pågældende udkast til retsakt. Hvis et ændringsforslag angår en eksisterende retsakt, som udkastet til retsakt har til formål at ændre, indeholder informationsblokken tillige en tredje og en fjerde linje, hvori det er anført, hvilken eksisterende retsakt og hvilken bestemmelse heri der er berørt.

Ændringsforslag fra Parlamentet i form af en konsolideret tekst

Ny tekst er markeret med ***fede typer og kursiv***. Tekst, som er bortfaldet, markeres med symbolet ▌ eller med overstregning. Ved udskiftninger markeres den nye tekst med ***fede typer og kursiv***, og den udskiftede tekst slettes eller overstreges.
Som en undtagelse bliver rent tekniske justeringer, der er foretaget af de berørte tjenestegrene med henblik på udarbejdelsen af den endelige tekst, ikke markeret.

INDHOLD

Side

FORSLAG TIL EUROPA-PARLAMENTETS LOVGIVNINGSMÆSSIGE BESLUTNING 5

BEGRUNDELSE....30

SKRIVELSE FRA UDVALGET OM DET INDRE MARKED OG FORBRUGERBESKYTTELSE....31

PROCEDURE I KORRESPONDERENDE UDVALG....36

ENDELIG AFSTEMNING VED NAVNEOPRÅB I KORRESPONDERENDE UDVALG .37

FORSLAG TIL EUROPA-PARLAMENTETS LOVGIVNINGSMÆSSIGE BESLUTNING

om forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester

(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Almindelig lovgivningsprocedure: førstebehandling)

Europa-Parlamentet,

– der henviser til Kommissionens forslag til Europa-Parlamentet og Rådet (COM(2023)0208),

– der henviser til artikel 294, stk. 2, og artikel 114 i traktaten om Den Europæiske Unions funktionsmåde, på grundlag af hvilke Kommissionen har forelagt forslaget for Parlamentet (C9-0137/2023),

– der henviser til artikel 294, stk. 3, i traktaten om Den Europæiske Unions funktionsmåde,

– der henviser til udtalelse af 13. juli 2023 fra Det Europæiske Økonomiske og Sociale Udvalg[1],

– der henviser til forretningsordenens artikel 59,

– der henviser til skrivelse fra Udvalget om det Indre Marked og Forbrugerbeskyttelse,

– der henviser til betænkning fra Udvalget om Industri, Forskning og Energi (A9-0307/2023),

1. vedtager nedenstående holdning ved førstebehandling;

2. anmoder om fornyet forelæggelse, hvis Kommissionen erstatter, i væsentlig grad ændrer eller agter i væsentlig grad at ændre sit forslag;

3. pålægger sin formand at sende Parlamentets holdning til Rådet og Kommissionen samt til de nationale parlamenter.

[1] EUT C 349 af 29.9.2023, s. 167.

Ændringsforslag 1

EUROPA-PARLAMENTETS ÆNDRINGSFORSLAG[*]

til Kommissionens forslag

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[2],

under henvisning til udtalelse fra Regionsudvalget,

efter den almindelige lovgivningsprocedure[3], og

---

[*] Ændringer: Ny eller ændret tekst er markeret med fede typer og kursiv; udgået tekst er markeret med symbolet ▌.

[2] ***EUT C 349 af 29.9.2023, s. 167.***

[3] ***Europa-Parlamentets holdning af … (endnu ikke offentliggjort i EUT) og Rådets afgørelse af ….***

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets forordning (EU) 2019/881[4] fastsætter en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for ***produkter inden for informations- og kommunikationsteknologi (IKT)***, IKT-tjenester og IKT-processer i Unionen samt at undgå fragmentering af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i Unionen.

(1a) For at sikre Unionens modstandsdygtighed over for cyberangreb og forhindre sårbarheder på EU-markedet er hensigten med denne forordning at supplere den horisontale lovramme, der fastsætter omfattende cybersikkerhedskrav for alle produkter med digitale elementer i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) .../...[5] (2022/0272(COD)), ved at opstille væsentlige krav til administrerede sikkerhedstjenester, deres anvendelse og deres pålidelighed.

(2) Administrerede sikkerhedstjenester, som er tjenester, der består i at udføre eller yde bistand til aktiviteter vedrørende kundernes risikostyring i forbindelse med cybersikkerhed, ***herunder forebyggelse, opdagelse og reaktion på eller genopretning efter hændelser,*** har fået stadig større betydning i forbindelse med forebyggelse og afbødning af cybersikkerhedshændelser. ***De aktiviteter, der udføres af udbydere af administrerede sikkerhedstjenester, består af tjenester vedrørende identificering, beskyttelse, opdagelse, reaktion og genopretning, herunder, men ikke begrænset til, levering af efterretninger om cybertrusler, overvågning af trusler i realtid ved hjælp af proaktive teknikker, herunder indbygget sikkerhed, risikovurdering, udvidet opdagelse, afhjælpning og reaktion.*** 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[6]. Det fremgår af direktivets betragtning 86, at udbydere af

---

4 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).

5 Europa-Parlamentets og Rådets forordning (EU) .../... af ... (EUT L, …, ELI: …).

6 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).

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 foretage genopretning 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, jf. 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 anvendes til at støtte foranstaltninger vedrørende indsats og 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 henhold til denne forordning.

(4) Certificering af administrerede sikkerhedstjenester er ikke kun relevant for udvælgelsesprocessen til EU's cybersikkerhedsreserve, men er 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 en 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.

(4a) Europæiske certificeringsordninger for administrerede sikkerhedstjenester bør føre til anvendelse af disse tjenester og til øget konkurrence på området under hensyntagen til både udbydernes og tjenestemodtagernes specifikke behov. Disse ordninger bør derfor ramme en balance mellem deres mål og den potentielle reguleringsmæssige, administrative og finansielle byrde, som udbydere, navnlig mikrovirksomheder eller små og mellemstore virksomheder (SMV'er), kan støde på. Desuden bør ordningerne tilskynde til anvendelse af certificerede administrerede sikkerhedstjenester ved at bidrage til tilgængeligheden heraf, navnlig for mindre aktører såsom mikrovirksomheder og SMV'er samt lokale og regionale myndigheder, der har begrænset kapacitet og begrænsede ressourcer, men som er mere udsatte for brud på cybersikkerheden med økonomiske, retlige, omdømmemæssige og operationelle konsekvenser.

(4b) Unionens certificeringsordning for administrerede sikkerhedstjenester bør tilsikre tilgængeligheden af sikre tjenester af høj kvalitet, som garanterer en sikker digital omstilling og bidrager til at nå de mål, der er fastsat i politikprogrammet "Vejen mod det digitale årti", navnlig med hensyn til målet om, at 75 % af EU's virksomheder skal begynde at anvende Cloud/AI/big data, at mere end 90 % af SMV'erne som minimum skal opnå et grundlæggende niveau af digital intensitet, og at centrale offentlige tjenester udbydes online.

(4c) I det nuværende digitale og teknologiske landskab, som er i hastig udvikling, varierer udbuddet af uddannelsesressourcer og formel uddannelse, og viden kan erhverves på forskellige måder, både formelle, f.eks. gennem universiteter eller kurser, og ikkeformelle, f.eks. gennem jobtræning eller langvarig erhvervserfaring inden for det relevante område.

(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 ***særlig*** certificeringsordning, er det derfor nødvendigt at ændre forordning (EU) 2019/881. ***Ved udviklingen af certificeringsordninger, der oprettes i henhold til denne forordning, bør der også tages hensyn til de resultater og anbefalinger, der kommer ud af den evaluering og revision, der er fastsat i forordningen.***

(5a) Med henblik på at lette fremvæksten af et pålideligt EU-marked og samtidig skabe partnerskaber med ligesindede tredjelande, herunder i lyset af bestemmelserne i Europa-Parlamentets og Rådets forordning (EU).../...[7] (2023/0109(COD)) med hensyn til adgang til EU's cybersikkerhedsreserve, bør den certificeringsproces, der etableres inden for rammerne af denne forordning, strømlines for at sikre international anerkendelse og tilpasning til internationale standarder.

(5b) Med henblik på at sikre udviklingen af et pålideligt EU-marked for administrerede sikkerhedstjenester bør udbyderne heraf og medlemsstaterne samarbejde og bidrage til indsamling af data om situationen og udviklingen på arbejdsmarkedet inden for cybersikkerhed.

(5c) En EU-dækkende koordineret tilgang til styrkelse af modstandsdygtigheden for kritisk infrastruktur er baseret på medlemsstaternes kapacitetsopbygning. Unionen står imidlertid over for en talentkløft, der er kendetegnet ved mangel på kvalificerede fagfolk, og et trusselsbillede i hastig udvikling som anerkendt i Kommissionens meddelelse af 18. april 2023 om EU's akademi for cybersikkerhedskompetencer. For at lette fremkomsten af væsentlige administrerede sikkerhedstjenester af høj kvalitet og for at få et bedre overblik over sammensætningen af Unionens arbejdsstyrke inden for cybersikkerhed bør samarbejdet mellem medlemsstaterne, Kommissionen, ENISA og interessenter, herunder den private sektor og den akademiske verden, derfor styrkes gennem udvikling af offentlig-private partnerskaber, støtte til forsknings- og innovationsinitiativer, udvikling og gensidig anerkendelse af fælles standarder for og certificering af cybersikkerhedsfærdigheder, bl.a. gennem den europæiske ramme for cybersikkerhedskompetencer. Dette bør også fremme

[7] Europa-Parlamentets og Rådets forordning (EU) .../... af ... (EUT L, …, ELI: …).

cybersikkerhedsfagfolks mobilitet inden for Unionen samt integration af viden om og uddannelse i cybersikkerhed i uddannelsesprogrammer, samtidig med at der sikres adgang til lærlingeuddannelser og praktikophold for unge, herunder personer, der bor i ugunstigt stillede regioner såsom øer, tyndt befolkede landdistrikter og fjerntliggende områder. Disse foranstaltninger bør også sigte mod at tiltrække flere kvinder og piger til dette emneområde og bidrage til at afhjælpe kønsskævheden inden for videnskab, teknologi, ingeniørvirksomhed og matematik. Den private sektor bør også tilstræbe at levere oplæring på arbejdspladsen med fokus på de mest efterspurgte kompetencer og inddrage offentlig forvaltning og nystartede virksomheder samt mikrovirksomheder og SMV'er.

(5d) Der bør sikres passende finansiering og ressourcer til de ekstra opgaver, som ENISA pålægges ved de ændringer af forordning (EU) 2019/881, der indføres ved nærværende forordning.

(5e) For at supplere visse ikkevæsentlige bestemmelser i denne forordning bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde med henblik på at fastlægge en europæisk cybersikkerhedscertificeringsordning for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning[8]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(5e) 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][9] —

---

[8] EUT L 123 af 12.5.2016, s. 1.

[9] ***EUT C .../…***

VEDTAGET DENNE FORORDNING:

Artikel 1

Ændring 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, IKT-processer og administrerede sikkerhedstjenester i Unionen samt at undgå fragmentering af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i Unionen."

2) I artikel 2 foretages følgende ændringer:

a) Nr. 9), 10) og 11) affattes således:

"9) "europæisk cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, som 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, som 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 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 ydet til en tredjepart

bestående i at udføre aktiviteter vedrørende styring af cybersikkerhedsrisici eller yde bistand til eller rådgivning om sådanne aktiviteter, herunder ***håndtering af*** 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, men 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) I artikel 8 foretages følgende ændringer:

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

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

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

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

b) Stk. 3 affattes således:

"3. ENISA udarbejder 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 foreskriver 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. ***I den forbindelse kan Kommissionen medtage en tilbundsgående vurdering af eksisterende uddannelsesforløb for at afhjælpe konstaterede kompetencekløfter og en liste med forslag til håndtering af behovene for kvalificerede medarbejdere og typer af kompetencer.***

3. Medtagelse af bestemte IKT-produkter, IKT-tjenester, IKT-processer eller kategorier heraf eller af administrerede sikkerhedstjenester i Unionens rullende arbejdsprogram skal være begrundet med udgangspunkt i 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 i relation til risikoen for fragmentering

b) relevant EU-ret eller national ret eller -politik

c) efterspørgslen på markedet

ca) den teknologiske udvikling og tilgængeligheden og udviklingen af internationale cybersikkerhedscertificeringsordninger og internationale og industrielle standarder

d) udviklingen i cybertrusselsbilledet

e) anmodning om, at ECCG udarbejder et specifikt forslag til ordning."

7) I artikel 49 ***foretages følgende ændringer***:

a) Stk. 7 affattes således:

*"*7. Kommissionen ***tillægges beføjelse til*** på grundlag af det af ENISA udarbejdede forslag til ordning ***at*** vedtage delegerede retsakter ***i overensstemmelse med artikel 65a for at supplere denne forordning ved at fastlægge en europæisk*** cybersikkerhedscertificeringsordning for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der opfylder kravene i artikel 51, 52 og 54."

b) Følgende stykke indsættes:

"7a. Inden vedtagelsen af sådanne delegerede retsakter gennemfører og offentliggør Kommissionen i samarbejde med ENISA en konsekvensanalyse af den foreslåede europæiske cybersikkerhedscertificeringsordning. I forbindelse med udarbejdelsen af konsekvensanalysen gennemfører Kommissionen offentlige høringer og hører SCCG og ECCG."

8) I artikel 51 foretages følgende ændringer:

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

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

f) at 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) at sikre, at de IKT-produkter, IKT-tjenester og IKT-processer, der anvendes til levering af administrerede sikkerhedstjenester, er sikre som følge af standardindstillinger og indbygget sikkerhed ***og er forsynet med ajourført software og hardware,*** ikke har kendte sårbarheder og omfatter de seneste sikkerhedsopdateringer."

10) I artikel 52 foretages følgende ændringer:

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 gennemgå."

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 konsekvenserne for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, som er blevet certificeret, eller for hvilke der er udstedt en EU-overensstemmelseserklæring, 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) I artikel 56 foretages følgende ændringer:

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 henhold til 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 obligatorisk 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 vurdering af denne art 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, navnlig under hensyntagen til foranstaltningens mulige indvirkning på producenter eller udbydere af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, herunder ***mikrovirksomheders og små og mellemstore virksomheders specifikke interesser og behov***."

iii) Følgende afsnit tilføjes:

"Med henblik på denne artikels tredje afsnit, litra d), sikrer Kommissionen passende finansiel støtte inden for de lovgivningsmæssige rammer for eksisterende EU-programmer, navnlig for at lette den finansielle byrde for mikrovirksomheder og SMV'er, herunder nystartede virksomheder, der opererer inden for administrerede sikkerhedstjenester."

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. Dette organ eller denne 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 ***delegerede retsakt***, som vedtages i henhold til 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) I artikel 58 foretages følgende ændringer:

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 områder, 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 områder, 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)".

16a) Følgende artikel indsættes:

"Artikel 65a
Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 49, stk. 7, tillægges Kommissionen for en periode på fem år fra den ... [datoen for den ændrede forordnings ikrafttræden]. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 49, stk. 7, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 49, stk. 7, træder kun i

kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med [to måneder] på Europa-Parlamentets eller Rådets initiativ."

17) Artikel 67 affattes således:

"Artikel 67

Evaluering og revision

1. Senest den 28. juni 2024 og hvert tredje år derefter vurderer Kommissionen virkningen og effektiviteten af ENISA's arbejde og af dets arbejdsmetoder, det eventuelle behov for at ændre ENISA's mandat og de finansielle virkninger af en sådan eventuel ændring. Evalueringen skal tage enhver tilbagemelding til ENISA som reaktion på dets aktiviteter i betragtning. Hvis Kommissionen finder, at der ikke længere er grund til at videreføre driften af ENISA i lyset af de mål, det mandat og de opgaver, som ENISA er tillagt, kan Kommissionen foreslå, at denne forordning ændres for så vidt angår de bestemmelser, der vedrører ENISA.

2. Evalueringen skal vurdere virkningen og effektiviteten af bestemmelserne i afsnit III i denne forordning med hensyn til målsætningerne om at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester i Unionen og forbedre det indre markeds funktion.

3. Evalueringen skal også vurdere:

a) effektiviteten af de procedurer, der fører til høring, forberedelse og vedtagelse af europæiske cybersikkerhedscertificeringsordninger, samt metoder til at forbedre og fremskynde disse procedurer

b) om der er behov for væsentlige cybersikkerhedskrav for adgang til det indre marked for at undgå, at IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der ikke opfylder

grundlæggende cybersikkerhedskrav, kommer ind på EU-markedet.

4. Senest den 28. juni 2024 og hvert tredje år derefter sender Kommissionen en rapport om evalueringen og dens konklusioner til Europa-Parlamentet, Rådet og bestyrelsen. Konklusionerne fra denne rapport offentliggøres."

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 hver medlemsstat.
Udfærdiget i …, den … .

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

BEGRUNDELSE

Ordføreren støtter forslaget til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) 2019/8811 for så vidt angår administrerede sikkerhedstjenester og forstår nødvendigheden af at ajourføre og styrke den europæiske cybersikkerhedscertificeringsordning ved at give mulighed for, at den omfatter vigtige og voksende tjenester i branchen. I betragtning af at de enkelte medlemsstater allerede er begyndt at vedtage certificeringsordninger for administrerede sikkerhedstjenester, er ordføreren af den opfattelse, at dette ændringsforslag til retsakten om cybersikkerhed er afgørende for at forhindre betydelige forskelle i de nationale ordninger, der ville resultere i en form for markedsfragmentering, som er i strid med Unionens økonomiske og strategiske interesser.

I den forbindelse anerkendes det, at planen er, at dette forslag skal supplere forordningen om cybersolidaritet, navnlig denne specifikke udvidelse af den europæiske cybersikkerhedscertificeringsordning, som vil gøre det muligt for administrerede sikkerhedstjenester – svarende til "betroede udbydere" i forordningen om cybersolidaritet – at spille en vigtig rolle i EU's fremtidige cybersikkerhedsreserve. Dette forslag er derfor også af stor betydning for at fremme en bredere EU-cybersikkerhedskapacitet, som er afgørende for at modvirke potentielle trusler i en geopolitisk virkelighed, der er i konstant udvikling.

Inden for rammerne af Kommissionens forslag er ordførerens mål at konsolidere denne målrettede ændring af forordningen om cybersikkerhed og skabe yderligere klarhed om den. Dette illustreres af ordførerens ændringer af definitionen af administrerede sikkerhedstjenester, der præciserer, at de er "outsourcet", samtidig med at det præciseres yderligere, hvad der kan indgå i definitionen. De fremsatte ændringsforslag vedrørende anerkendelse af internationale cybersikkerhedsstandarder har til formål at fremme en højere grad af tillid og samtidig udvikle udførlige EU-regler.

I dette udkast til betænkning lægges der større vægt på at afhjælpe kompetencekløften og støtte mikrovirksomheder og små og mellemstore virksomheder. Med hensyn til førstnævnte bygger de fremsatte ændringsforslag på den allerede implicitte nødvendighed af færdigheder i cybercertificeringsordningen vis-à-vis "den nødvendige kompetence, ekspertise og erfaring af personale med et meget højt niveau af relevant teknisk viden og faglig integritet". Efter ordførerens opfattelse skal den europæiske certificeringsordning, samtidig med at den fremmer samarbejdet mellem alle involverede aktører og mellem medlemsstaterne, den private sektor, den akademiske verden og forskningsinstitutioner, fungere som en katalysator for en ny køreplan for uddannelse og styrkelse af arbejdsstyrken, indsamling af flere data om de kompetencer, der er behov for, og bidrag med henblik på at afhjælpe kønsskævheden inden for STEM.

Samtidig bør mikrovirksomheder og små og mellemstore virksomheder, som udgør rygraden i den europæiske økonomi og bestemt har en positiv rolle at spille i cybersikkerhedsbranchen, nyde godt af passende finansiel støtte inden for lovrammerne for eksisterende EU-programmer for at lette en eventuel uforholdsmæssigt stor økonomisk byrde, der pålægges dem.

21.9.2023

SKRIVELSE FRA UDVALGET OM DET INDRE MARKED OG FORBRUGERBESKYTTELSE

Cristian Silviu Buşoi
Formand
Udvalget om Industri, Forskning og Energi
BRUXELLES

Om: Udtalelse om forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Kære formand

I forbindelse med ovennævnte procedure er Udvalget om det Indre Marked og Forbrugerbeskyttelse blevet anmodet om at afgive en udtalelse til Deres udvalg. På mødet den 23. maj 2023 vedtog udvalget at sende denne udtalelse i form af en skrivelse. Udvalget behandlede spørgsmålet på mødet den 19. september 2023 og vedtog udtalelsen på samme møde.

På dette møde[1] vedtog det at opfordre Udvalget om Industri, Forskning og Energi (ITRE), som er korresponderende udvalg, til at optage nedenstående forslag i det beslutningsforslag, det vedtager.

Med venlig hilsen

Anna Cavazzini

[1] Til stede ved den endelige afstemning: Anna Cavazzini (formand), Andrus Ansip (næstformand), Krzysztof Hetman (næstformand), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

FORSLAG

Udvalget om det Indre Marked og Forbrugerbeskyttelse opfordrer Udvalget om Industri, Forskning og Energi, som er korresponderende udvalg, til at tage hensyn til følgende forslag:

A. der henviser til, at Kommissionen den 18. april 2023 offentliggjorde et lovgivningsforslag om administrerede sikkerhedstjenester, der indebærer målrettede ændringer af EU's forordning om cybersikkerhed[2];

B. der henviser til, at Udvalget om det Indre Marked og Forbrugerbeskyttelse (IMCO) i forbindelse med lovgivningsforslaget til EU's forordning om cybersikkerhed (2017/0225 (COD))[3] forelagde en udtalelse i henhold til forretningsordenens artikel 54 for det ansvarlige Udvalg om Industri, Forskning og Energi (ITRE) med delte kompetencer vedrørende rammen for cybersikkerhedscertificering i betragtning af IMCO's klare kompetence med hensyn til certificeringsordninger og, i almindelighed, standardisering, markedsovervågning og gennemførelse af det digitale indre marked;

C. der henviser til, at EU's forordning om cybersikkerhed[4] har til formål at opnå 1) et højt niveau af cybersikkerhed, cyberrobusthed og tillid i EU ved at fastsætte mål, opgaver og organisatoriske forhold for et styrket agentur omdøbt til Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) med et nyt permanent mandat og 2) en ramme for frivillige europæiske cybersikkerhedscertificeringsordninger for produkter, tjenester og processer inden for informations- og kommunikationsteknologi (IKT);

D. der henviser til de foreslåede målrettede ændringer med henblik på at medtage administrerede sikkerhedstjenester i anvendelsesområdet for EU's forordning om cybersikkerhed og tilføje en definition af de tjenester, der er nøje tilpasset definitionen i NIS 2-direktivet[5]; der henviser til, at ændringerne vil sætte Kommissionen i stand til ved hjælp af gennemførelsesretsakter at vedtage europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester i lighed med IKT-produkter, -tjenester og -processer, som allerede er omfattet af forordningen om cybersikkerhed;

E. der henviser til, at administrerede sikkerhedstjenester spiller en stadig vigtigere rolle i forbindelse med forebyggelse og afbødning af cybersikkerhedshændelser;

1. anerkender, at Rådet den 23. maj 2022[6] opfordrede til en forøgelse af det overordnede cybersikkerhedsniveau i EU ved at lette fremkomsten og udviklingen af betroede udbydere af cybersikkerhedstjenester; mener, at bl.a. krigen i Ukraine, den nuværende geopolitiske kontekst og de fortsatte trusler fra tredjelandes ordninger samt et stadigt voksende marked for digitale teknologier og digital omstilling af processer generelt har ført til behovet for et højere cybersikkerhedsniveau i EU og dets medlemsstater; anbefaler, at Kommissionen træffer proaktive foranstaltninger for at støtte udviklingen

[2] https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:52023PC0208
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)
[4] EUT L 151 af 7.6.2019, s. 15.
[5] EUT L 333 af 27.12.2022, s. 80.
[6] 9364/22

af betroede udbydere af cybersikkerhedstjenester såsom finansiering af forskning og udvikling, uddannelsesprogrammer til opbygning af cybersikkerhedskompetencer og incitamenter for virksomheder til at investere i cybersikkerhed; foreslår, at EU styrker sit samarbejde med NATO og andre internationale partnere for at reagere på cybertrusler fra tredjelandes ordninger, herunder udveksling af trusselsefterretninger, fælles øvelser og koordinerede reaktioner på cyberangreb;

2. understreger, at certificering af administrerede sikkerhedstjenester, der er baseret på ikkediskriminerende regler og afspejler europæiske og internationale standarder, er afgørende for at opbygge og sikre tillid til kvaliteten af disse tjenester, navnlig med henblik på at opnå et højt forbrugerbeskyttelsesniveau; bemærker, at nogle medlemsstater allerede har vedtaget certificeringsordninger for administrerede sikkerhedstjenester, og at det derfor er afgørende at undgå fragmentering af det indre marked og uoverensstemmelser, som kan påvirke cybersikkerhedsindustrien og -virksomhederne, og at muliggøre en harmoniseret tilgang gennem oprettelse af en europæisk cybersikkerhedscertificeringsordning for sådanne tjenester; anmoder om, at rammen for cybersikkerhedscertificering bør omfatte bedste praksis fra eksisterende nationale certificeringsordninger og udvikles i samråd med centrale interessenter i cybersikkerhedsindustrien;

3. fremhæver, at udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand spiller en vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser; mener, at eftersom flere og flere virksomheder kæmper for at opretholde forskellige komplekse softwaresystemer og sammenkoblede virksomhedsnetværk, er de nødvendigvis afhængige af udbydere af administrerede sikkerhedstjenester, og at sådanne udbydere derfor bør betragtes som et væsentligt element i EU's cybersikkerhedsøkosystem; bemærker imidlertid, at udbydere af administrerede sikkerhedstjenester også selv har været mål for cyberangreb og kan udgøre en særlig risiko på grund af deres tætte integration i kundernes aktiviteter.

4. minder om betydningen af det nyligt vedtagne NIS 2-direktiv for at sikre et højere niveau af cyberrobusthed i hele Unionen; opfordrer til en hurtig vedtagelse og gennemførelse af gennemførelsesretsakter i henhold til dette direktiv for at sikre, at udbydere af administrerede sikkerhedstjenester overholder direktivets krav til foranstaltninger til styring af cybersikkerhedsrisici;

5. anbefaler, at udbydere af administrerede sikkerhedstjenester bør forpligtes til at overholde relevante cybersikkerhedsstandarder og gennemgå regelmæssige revisioner med henblik på at sikre, at deres systemer er sikre for ikke blot at beskytte udbyderne selv, men også de enheder, de betjener; mener, at sådanne revisioner bør vurdere udbydernes overholdelse af den EU-dækkende ramme for cybersikkerhedscertificering og deres evne til at beskytte både deres og deres kunders systemer mod cybertrusler;

6. glæder sig over lovgivningsforslaget om administrerede sikkerhedstjenester, som har til formål at forbedre kvaliteten af administrerede sikkerhedstjenester og øge deres sammenlignelighed til gavn for et velfungerende indre marked og gennemførelsen af det digitale indre marked; understreger, at certificering af administrerede sikkerhedstjenester er relevant for udvælgelsesprocessen til EU's

cybersikkerhedsreserve og også er en vigtig kvalitets- og tillidsindikator for private og offentlige enheder, der har til hensigt at købe sådanne tjenester;

7. bemærker, at forslaget styrker ENISA's rolle, som bør støtte og fremme udviklingen og gennemførelsen af Unionens politik for cybersikkerhedscertificering af IKT-produkter, -tjenester, -processer og administrerede sikkerhedstjenester ved regelmæssigt at overvåge udviklingen inden for relaterede standardiseringsområder og anbefale tekniske specifikationer, hvor der ikke findes standarder; foreslår, at ENISA tildeles yderligere ressourcer og beføjelser til at varetage sin udvidede rolle, herunder finansiering af forskning og udvikling, og et klart mandat til at koordinere med nationale cybersikkerhedsagenturer og interessenter fra industrien; understreger den afgørende rolle, som enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), spiller med hensyn til at skabe et forudsigeligt og sikkert digitalt rum for virksomheder og borgere;

8. opfordrer Kommissionen og ENISA til at støtte og sikre en konsekvent gennemførelse af den europæiske cybersikkerhedscertificeringsordning, der er baseret på ikkediskriminerende regler og afspejler europæiske og internationale standarder for selvvurdering af overensstemmelse foretaget af producenten eller udbyderen af IKT-produkter, -tjenester, -processer eller administrerede sikkerhedstjenester i overensstemmelse med EU's forordning om cybersikkerhed; mener, at gennemførelsen bør bidrage til at udligne omkostningerne ved akkreditering og tilskynde flere producenter eller udbydere til at deltage i ordningen;

9. understreger, at hver enkelt certificeringsordning udformes på en måde, der opmuntrer og tilskynder alle aktører, der er involveret i den pågældende sektor, til at udvikle og vedtage regelmæssigt ajourførte sikkerhedsstandarder, tekniske normer og principper om indbygget sikkerhed og privatlivsbeskyttelse for alle faser af produkternes eller tjenesteydelsernes livscyklus; fremhæver, at input fra civilsamfundet, uafhængige sikkerhedsforskere og andre relevante interessenter skal tages i betragtning på en mere systematisk måde, når sådanne principper udvikles; mener, at certificeringsordningerne bør være i overensstemmelse med andre europæiske cybersikkerhedscertificeringsordninger, der vedtages i overensstemmelse med EU's forordning om cybersikkerhed, og bør udformes så de ikke medfører en uforholdsmæssig stor byrde for udbyderne; anbefaler, at certificeringsordninger bør omfatte klare og detaljerede retningslinjer for, hvordan principperne om indbygget sikkerhed og indbygget privatlivsbeskyttelse kan gennemføres, når sådanne retningslinjer er i overensstemmelse med bestemmelserne om rammerne for europæiske cybersikkerhedsordninger i EU's forordning om cybersikkerhed; foreslår, at certificeringsordninger, hvor det er nødvendigt og forholdsmæssigt, bør bestå af en mekanisme til løbende forbedring såsom regelmæssige revisioner og ajourføringer af sikkerhedsstandarder og tekniske normer; mener, at mekanismen bør tage hensyn til den seneste udvikling inden for cybersikkerhedstrusler og -teknologier; tilskynder til, at hver certificeringsordning bør omfatte foranstaltninger til fremme af gennemsigtighed og ansvarlighed, såsom offentliggørelse af certificeringsresultater og sanktioner for manglende overholdelse;

10. opfordrer til, at der indføres et frivilligt EU-tillidsmærke for certificerede IKT-produkter, -tjenester, -processer og administrerede sikkerhedstjenester; fremhæver i denne forbindelse, at mærket kan bidrage til at øge bevidstheden om cybersikkerhed i

hele det indre marked og give virksomheder med gode cybersikkerhedsoplysninger en konkurrencefordel; foreslår, at EU-tillidsmærket udformes, så det er let genkendeligt og forståeligt for forbrugere og virksomheder;

11. anbefaler Kommissionen og ENISA at oprette et særligt forsknings- og udviklingsprogram for cybersikkerhed; anbefaler, at Kommissionen og ENISA etablerer en ramme for risikovurdering af cybersikkerhed for virksomheder med retningslinjer for, hvordan cybersikkerhedsrisici identificeres, vurderes og afbødes, og som kan skræddersys til forskellige sektorer og størrelser af virksomheder; foreslår, at Kommissionen og ENISA tilbyder medlemsstaterne hjælp og bistand til at etablere en mekanisme til indberetning af cybersikkerhedshændelser for forbrugere og virksomheder med henblik på at lette indsamlingen af data om cybersikkerhedshændelser, som kan anvendes til at forbedre cybersikkerhedspolitikker og -praksis.

PROCEDURE I KORRESPONDERENDE UDVALG

Titel	om ændring af forordning (EU) 2019/881 for så vidt angår administrerede sikkerhedstjenester
Referencer	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Dato for forelæggelse for EP	19.4.2023
Korresponderende udvalg Dato for vedtagelse	ITRE 1.6.2023
Rådgivende udvalg Dato for vedtagelse	IMCO LIBE 1.6.2023 1.6.2023
Ingen udtalelse Dato for afgørelse	LIBE 30.5.2023
Ordførere Dato for valg	Josianne Cutajar 2.5.2023
Behandling i udvalg	19.7.2023 19.9.2023
Dato for vedtagelse	25.10.2023
Resultat af den endelige afstemning	+: 57 –: 0 0: 2
Til stede ved den endelige afstemning – medlemmer	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Til stede ved den endelige afstemning – stedfortrædere	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Til stede ved den endelige afstemning – stedfortrædere (forretningsordenens art. 209, stk. 7)	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Dato for indgivelse	26.10.2023

ENDELIG AFSTEMNING VED NAVNEOPRÅB
I KORRESPONDERENDE UDVALG

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller