Europa-Parlamentet
2019-2024

Udvalget om Industri, Forskning og Energi

2023/0108(COD)

21.9.2023

ÆNDRINGSFORSLAG
17 - 52

Udkast til betænkning
Josianne Cutajar
(PE752.802v01-00)

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

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

Ændringsforslag 17
Evžen Tošenovský

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(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 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.	***(2)*** Administrerede sikkerhedstjenester er tjenester, der ***udføres af udbydere af administrerede sikkerhedstjenester i henhold til artikel 6, nr. 40), i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555. Disse tjenester*** består i at udføre eller yde bistand til aktiviteter vedrørende kundernes risikostyring i forbindelse med cybersikkerhed, ***og*** har fået stadig større betydning i forbindelse med forebyggelse og afbødning af cybersikkerhedshændelser. Udbydere af ***administrerede sikkerhedstjenester*** anses derfor for at være væsentlige eller vigtige enheder, der tilhører en sektor af særlig kritisk betydning i henhold til ***nr. 10), i bilag I i*** 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.
[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	[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).

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).

Or. en

Ændringsforslag 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(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 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	(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 af hændelser, opdagelse og reaktion eller reetablering,*** 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 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

sikkerhedstjenester.	forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.
[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).	[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).

Or. en

Ændringsforslag 19
Evžen Tošenovský

Forslag til forordning
Betragtning 3

Kommissionens forslag	*Ændringsforslag*
(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***	(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 ***betroede*** udbydere ***af administrerede sikkerhedstjenester***, der udgør EU's cybersikkerhedsreserve, som bl.a. bør tage hensyn til, om den pågældende udbyder har opnået en

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***.

europæisk eller national cybersikkerhedscertificering. ***Når der er indført en europæisk cybersikkerhedscertificeringsordning for administrerede sikkerhedstjenester, som også vil erstatte alle relevante nationale cybersikkerhedscertificeringsordninger, bør en obligatorisk certificering*** i ***overensstemmelse med denne certificeringsordning desuden finde anvendelse*** på ***medtagelse af betroede udbydere af administrerede sikkerhedstjenester*** i ***EU's cybersikkerhedsreserve***.

Or. en

Ændringsforslag 20
Johan Nissinen

Forslag til forordning
Betragtning 4

Kommissionens forslag	*Ændringsforslag*
(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.	(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. ***Samtidig bør disse mange formål med forordningen skabe en balance i forhold til den potentielle reguleringsmæssige byrde og de potentielle omkostninger i forbindelse***

med certificering, eftersom overholdelse af certificeringskravene vil medføre yderligere udgifter og administrative udfordringer, hvilket kan være et problem for mindre udbydere.

Or. en

Ændringsforslag 21
Ville Niinistö
for Verts/ALE-Gruppen

Forslag til forordning
Betragtning 4 a (ny)

Kommissionens forslag	*Ændringsforslag*
	4a) Eftersom markedet og uddannelsessystemerne tilbyder en bred vifte af uddannelsesressourcer og formel uddannelse, skal det understreges, at viden også kan opnås på ikkeformelle måder, og at færdigheder kan påvises gennem eksamensbeviser og certificering, men ikke udelukkende. Navnlig i det aktuelle hurtigt skiftende trusselsbillede bør medlemsstaterne og modtagerne af administrerede sikkerhedstjenester tage hensyn til højt kvalificerede sårbarhedsforskere. Desuden kan enheder og fysiske personer, der forsker i sårbarheder, i nogle medlemsstater blive udsat for strafferetligt og civilretligt ansvar, og medlemsstaterne opfordres derfor til at udstede retningslinjer for ikke-retsforfølgelse af forskning i informationssikkerhed og en fritagelse for civilretligt ansvar for disse aktiviteter.

Or. en

Begrundelse

Sikkerhedspersonalets landskab varierer til dels på grund af forskellige ikke-standardiserede karriereforløb, adgang til formel uddannelse og ressourcer til at blive certificeret. Vi er derfor nødt til at tilskynde til beskæftigelse af kvalificerede personer og sikre en positiv ramme for aktiviteter, der resulterer i en forbedring af cybersikkerheden.

Ændringsforslag 22
Josianne Cutajar

Forslag til forordning
Betragtning 4 a (ny)

Kommissionens forslag	*Ændringsforslag*
	4a) Unionens certificeringsordning for administrerede sikkerhedstjenester bør sikre 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[8a]", 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.
	8a Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030.

Or. en

Ændringsforslag 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 4 a (ny)

Kommissionens forslag	*Ændringsforslag*
	4a) De europæiske certificeringsordninger for administrerede sikkerhedstjenester bør lette anvendelsen af disse tjenester, navnlig for mindre enheder, herunder lokale og regionale

myndigheder eller SMV'er, som ofte ikke har den finansielle og menneskelige kapacitet til selv at udføre disse tjenester, men som er sårbare over for cyberangreb med potentielt betydelige konsekvenser.

Or. en

Ændringsforslag 24
Josianne Cutajar

Forslag til forordning
Betragtning 5

Kommissionens forslag	*Ændringsforslag*
(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] —	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 ***certificeringsordning, der oprettes i henhold til denne forordning, bør også tage hensyn til resultaterne og anbefalingerne fra den evaluering og revision, der er omhandlet i forordningens artikel 67. 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] —

Or. en

Ændringsforslag 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 5

Kommissionens forslag	*Ændringsforslag*
(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] —	(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 ***og pålidelighed af*** 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] —

Or. en

Ændringsforslag 26
Evžen Tošenovský

Forslag til forordning
Betragtning 5

Kommissionens forslag	*Ændringsforslag*
(5) Ud over udbredelsen af IKT-produkter, IKT-tjenester eller IKT-processer leverer administrerede sikkerhedstjenester ofte yderligere servicefunktioner, der afhænger af	(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] —	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. 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] —

Or. en

Ændringsforslag 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 5 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(5a) Eftersom de europæiske cybersikkerhedsordninger bør certificere, at administrerede sikkerhedstjenester leveres af højt kvalificeret personale, der er i stand til på pålidelig vis at levere disse tjenester og sikre de højeste standarder for cybersikkerhed, er det afgørende, at der er tilstrækkeligt udbud af højt kvalificeret personale i Unionen. 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. Det er vigtigt at bygge bro over denne talentkløft ved at styrke samarbejdet og

koordineringen mellem de forskellige interessenter, herunder den private sektor, den akademiske verden, medlemsstaterne, Kommissionen og ENISA, for at opskalere og skabe synergier for investeringer i uddannelse, udvikling af offentlig-private partnerskaber, støtte til forsknings- og innovationsinitiativer, udvikling og gensidig anerkendelse af fælles standarder og certificering af cybersikkerhedskompetencer, herunder gennem den europæiske ramme for cybersikkerhedskompetencer. Dette bør også fremme mobiliteten for fagfolk inden for cybersikkerhed i Unionen.

Or. en

Ændringsforslag 28
Johan Nissinen

Forslag til forordning
Betragtning 5 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(5a) Eftersom certificeringsordninger vil gøre et allerede komplekst lovgivningsmæssigt landskab mere komplekst, er det af afgørende betydning at forhindre potentielle overlapninger eller konflikter med eksisterende cybersikkerhedsregler og -standarder. Gennemførelsen af forordningen kræver desuden nøje overvejelse og proportionalitet med henblik på at mindske de negative virkninger på markedsfriheden og innovationen.

Or. en

Ændringsforslag 29
Josianne Cutajar

Forslag til forordning
Betragtning 5 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(5a) Der bør overvejes passende finansiering og ressourcer til at ledsage de yderligere opgaver, som ENISA pålægges ved denne forordning.

Or. en

Ændringsforslag 30
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra a – indledning

Kommissionens forslag	*Ændringsforslag*
a) Nr. 9, 10 og 11 affattes således:	a) Nr. ***7,*** 9, 10 og 11 affattes således:

Or. en

Ændringsforslag 31
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra a
Forordning (EU) nr. 2019/881
Artikel 2 – nr. 7

Kommissionens forslag	*Ændringsforslag*
	7) "håndtering af hændelser": håndtering af hændelser som defineret i artikel 6, nr. 8), i direktiv (EU) 2022/2555

Or. en

Ændringsforslag 32
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra b – indledning

Kommissionens forslag	*Ændringsforslag*
b) Følgende ***nummer*** indsættes:	b) Følgende ***numre*** indsættes:

Or. en

Ændringsforslag 33
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra b
Forordning (EU) nr. 2019/881
Artikel 2 – nr. 7 a

Kommissionens forslag	*Ændringsforslag*
	7a) "risiko": en risiko som defineret i artikel 6, nr. 9), i direktiv (EU) 2022/2555.

Or. en

Ændringsforslag 34
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra b
Forordning (EU) nr. 2019/881
Artikel 2 – nr. 14a

Kommissionens forslag	*Ændringsforslag*
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"***	14a) "administreret sikkerhedstjeneste": en ***administreret sikkerhedstjeneste som defineret i artikel 6***, ***nr. 40)***, ***i direktiv (EU) 2022/2555***

Or. en

Ændringsforslag 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra b
Forordning (EU) nr. 2019/881
Artikel 2 – nr. 14a

Kommissionens forslag	*Ændringsforslag*
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"***	14a) "administreret sikkerhedstjeneste": en ***administreret*** tjeneste, der består i at udføre aktiviteter vedrørende styring af cybersikkerhedsrisici eller yde bistand til sådanne aktiviteter, herunder ***forebyggelse, opdagelse,*** reaktion ***eller reetablering i forbindelse med hændelser***

Or. en

Ændringsforslag 36
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 2 – litra b
Forordning (EU) nr. 2019/881
Artikel 2 – nr. 14aa

Kommissionens forslag	*Ændringsforslag*
	14aa) "udbyder af administrerede sikkerhedstjenester": en udbyder af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555

Or. en

Ændringsforslag 37
Ville Niinistö
for Verts/ALE-Gruppen

Forslag til forordning
Artikel 1 – stk. 1 – nr. 6
Forordning (EU) nr. 2019/881
Artikel 47 – stk. 2

Kommissionens forslag	*Ændringsforslag*
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.	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. ***Støtteforanstaltninger til vurdering af faglærte medarbejderes behov, typer af færdigheder og eksisterende uddannelsesforløb skal medtages sammen med foranstaltninger til at afhjælpe eventuelle konstaterede mangler.***

Or. en

Begrundelse

Arbejdet med at identificere IKT-produkter, -tjenester og -processer eller kategorier heraf og administrerede sikkerhedstjenester skal ledsages af en færdighedsvurdering og foranstaltninger til at afhjælpe manglerne.

Ændringsforslag 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Forslag til forordning
Artikel 1 – stk. 1 – nr. 6
Forordning (EU) nr. 2019/881
Artikel 47 – stk. 3 – litra a

Kommissionens forslag	*Ændringsforslag*
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	a) tilgængeligheden og udviklingen af nationale cybersikkerhedscertificeringsordninger ***og internationale standarder og industristandarder***, der omfatter en bestemt kategori af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, og

navnlig for så vidt angår risikoen for fragmentering

Or. en

Begrundelse

Unionens rullende arbejdsprogram bør ikke kun vurdere udviklingen af nationale ordninger, men også industristandarder og internationale standarder.

Ændringsforslag 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 7
Forordning (EU) nr. 2019/881
Artikel 49 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7) Artikel 49, stk. 7, affattes således:	***udgår***
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.".	

Or. en

Ændringsforslag 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Forslag til forordning
Artikel 1 – stk. 1 – nr. 7
Forordning (EU) nr. 2019/881
Artikel 49 – stk. 7

Kommissionens forslag	*Ændringsforslag*
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.".***	7. Kommissionen kan på grundlag af det af ENISA udarbejdede forslag til ordning vedtage ***delegerede retsakter*** vedrørende europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der opfylder kravene i artikel 51, 52 og 54.
	(Dette ændringsforslag gælder for hele teksten. Hvis det vedtages, skal ændringerne foretages alle relevante steder).

Or. en

Ændringsforslag 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Forslag til forordning
Artikel 1 – stk. 1 – nr. 7
Forordning (EU) nr. 2019/881
Artikel 49 – stk. 7 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	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 høringer af Cybersikkerhedscertificeringsgruppen for Interessenter og Den Europæiske Cybersikkerhedscertificeringsgruppe.

Or. en

Ændringsforslag 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 7 a (nyt)
Forordning (EU) nr. 2019/881
Artikel 49 – stk. 7 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	7a) Følgende stykke indsættes:
	"7a. Kommissionen kan på grundlag af det af ENISA udarbejdede forslag til ordning vedtage delegerede retsakter vedrørende europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester, der opfylder kravene i artikel 51, 52 og 54. Disse delegerede retsakter vedtages efter proceduren i artikel 66a."

Or. en

Ændringsforslag 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 9
Forordning (EU) nr. 2019/881
Artikel 51a – stk. 1 – litra b

Kommissionens forslag	*Ændringsforslag*
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***	b) sikre, at udbyderen har indført passende interne procedurer til at sikre, at de administrerede sikkerhedstjenester til enhver tid leveres på et meget højt ***niveau af kvalitet og pålidelighed***

Or. en

Ændringsforslag 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 9
Forordning (EU) nr. 2019/881
Artikel 51a – stk. 1 – litra g

Kommissionens forslag	*Ændringsforslag*
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."	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, ***er forsynet med ajourført software og hardware,*** ikke har kendte sårbarheder og omfatter de seneste sikkerhedsopdateringer."

Or. en

Ændringsforslag 45
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 9
Forordning (EU) nr. 2019/881
Artikel 51a – stk. 1 – litra g

Kommissionens forslag	*Ændringsforslag*
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."	g) 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, ikke har kendte sårbarheder og omfatter de seneste sikkerhedsopdateringer."

Or. en

Ændringsforslag 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 13 – litra b – nr. ii – litra aa
Forordning (EU) nr. 2019/881
Artikel 56 – stk. 3 – afsnit 3 – litra a

Kommissionens forslag	*Ændringsforslag*
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*"*	a) tage hensyn til foranstaltningernes indvirkning på producenter og udbydere af sådanne IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester 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***, herunder SMV'er. Kommissionen sikrer, at SMV'er har adgang til passende finansiel støtte til gennemførelsen af foranstaltningerne gennem allerede eksisterende EU-programmer***

Or. en

Ændringsforslag 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Forslag til forordning
Artikel 1 – stk. 1 – nr. 14
Forordning (EU) nr. 2019/881
Artikel 57 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der er	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.	omfattet af en europæisk cybersikkerhedscertificeringsordning, ophører med at have virkning fra det tidspunkt, der fastsættes i den ***delegerede retsakt***, 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. *(Dette ændringsforslag gælder for hele teksten. Hvis det vedtages, skal ændringerne foretages alle relevante steder).*

Or. en

Begrundelse

Dette afspejler ændringsforslaget til artikel 49.

Ændringsforslag 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 1 – stk. 1 – nr. 16 a (nyt)
Forordning (EU) nr. 2019/881
Artikel 66 a (ny)

Kommissionens forslag	*Ændringsforslag*
	16a) Følgende artikel indsættes:
	Artikel 66a (ny)
	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. 7a, tillægges

Kommissionen for en periode på 5 år fra den ... [datoen for den lovgivningsmæssige basisretsakts ikrafttræden eller enhver anden dato fastsat af de to lovgivere]. 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. 7a, 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 om bedre lovgivning af 13. april 2016.

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. 7a, 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.

Or. en

Ændringsforslag 49
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 17 – indledning
Forordning (EU) nr. 2019/881
Artikel 67

Kommissionens forslag	*Ændringsforslag*
17) Artikel 67, stk. ***2*** og ***3***, affattes således:	***(***17) Artikel 67, stk. ***1, 2, 3*** og ***4***, affattes således:

Or. en

Ændringsforslag 50
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 17
Forordning (EU) nr. 2019/881
Artikel 67 – stk. 1

Kommissionens forslag	*Ændringsforslag*
	1 Senest den 28. juni 2024 og hvert fjerde år derefter vurderer Kommissionen virkningen og effektiviteten af ENISA's arbejde og af dets arbejdsmetoder, et eventuelt behov for at ændre ENISA's mandat og de finansielle virkninger af en sådan eventuel ændring. Evalueringen skal tage hensyn til enhver tilbagemelding til ENISA som reaktion på dets aktiviteter. 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 med hensyn til de bestemmelser, der vedrører ENISA.

Or. en

Ændringsforslag 51
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 17
Forordning (EU) nr. 2019/881
Artikel 67 – stk. 2

Kommissionens forslag	*Ændringsforslag*
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.	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***, herunder vurdering af den procedure og de tidsfrister, der fører til udarbejdelse og vedtagelse af de første europæiske cybersikkerhedscertificeringsordninger, og hvordan denne procedure kan forbedres og fremskyndes for efterfølgende certificeringsordninger***.

Or. en

Ændringsforslag 52
Evžen Tošenovský

Forslag til forordning
Artikel 1 – stk. 1 – nr. 17
Forordning (EU) nr. 2019/881
Artikel 67 – stk. 4

Kommissionens forslag	*Ændringsforslag*
	4. Senest den 28. juni 2024 og hvert fjerde år derefter sender Kommissionen en rapport om evalueringen og dens konklusioner til Europa-Parlamentet, Rådet og bestyrelsen. Resultaterne i denne rapport offentliggøres. Rapporten ledsages om nødvendigt af et lovgivningsforslag.

Or. en