2025/37

15.1.2025

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2025/37

af 19. december 2024

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 ([1]),

under henvisning til udtalelse fra Regionsudvalget,

efter den almindelige lovgivningsprocedure ([2]), og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([3]) 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.

(2) For at sikre Unionens modstandsdygtighed over for cyberangreb og forhindre sårbarheder på det indre marked er hensigten med denne forordning at supplere den horisontale lovramme, der fastsætter omfattende cybersikkerhedskrav for alle produkter med digitale elementer i henhold til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 ([4]), ved at fastlægge sikkerhedsmålsætninger for administrerede sikkerhedstjenester såvel som til anvendelsen og pålideligheden af disse tjenester.

(3) Administrerede sikkerhedstjenester udføres af udbydere af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([5]). Definitionen af »administrerede sikkerhedstjenester« i denne forordning bør derfor være i overensstemmelse med definitionen af »udbydere af administrerede sikkerhedstjenester« i 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 hændelser. Udbydere af disse tjenester anses derfor for at være væsentlige eller vigtige enheder, der tilhører en sektor af særlig kritisk betydning i henhold til direktiv (EU) 2022/2555. Som det fremgår af direktivets betragtning 86 spiller udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser. Imidlertid har udbydere af administrerede sikkerhedstjenester også selv været mål for cyberangreb og udgør en særlig risiko på grund af deres tætte integration i kundernes aktiviteter. Det er derfor vigtigt at væsentlige og vigtige enheder i henhold til direktiv (EU) 2022/2555 udviser forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.

([1]) EUT C 349 af 29.9.2023, s. 167.
([2]) Europa-Parlamentets holdning af 24.4.2024 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 2.12.2024.
([3]) 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).
([4]) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) 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).

(4) Definitionen af administrerede sikkerhedstjenester i henhold til denne forordning omfatter en ikkeudtømmende liste over administrerede sikkerhedstjenester, der kan komme i betragtning til europæiske cybersikkerhedscertificeringsordninger, såsom håndtering af hændelser, penetrationstest, sikkerhedsrevisioner og konsulentbistand vedrørende teknisk støtte. Administrerede sikkerhedstjenester kan omfatte cybersikkerhedstjenester, der støtter beredskab vedrørende forebyggelse af, opdagelse af, analyse af, afbødning af og reaktion på og genopretning efter hændelser. Levering af efterretninger om cybertrusler og risikovurdering i forbindelse med teknisk støtte kan også betragtes som administrerede sikkerhedstjenester. Der kan være separate sikkerhedsmålsætninger for europæiske cybersikkerhedscertificeringsordninger for forskellige administrerede sikkerhedstjenester. De europæiske cybersikkerhedsattester, der udstedes i overensstemmelse med sådanne ordninger, bør henvise til specifikke administrerede sikkerhedstjenester fra en specifik udbyder af disse tjenester.

(5) Udbydere af administrerede sikkerhedstjenester kan også spille en vigtig rolle i forbindelse med EU-foranstaltninger til støtte for indsats og en første genopretning i tilfælde af væsentlige hændelser og omfattende cybersikkerhedshændelser, der er afhængige af tjenester fra betroede private udbydere og afprøvning af kritiske enheder for potentielle sårbarheder baseret på sikkerhedsrisikovurderinger på EU-plan. Certificeringen af administrerede sikkerhedstjenester kan spille en rolle i udvælgelsen af betroede udbydere af administrerede sikkerhedstjenester som defineret i Europa-Parlamentets og Rådets forordning (EU) 2025/38 ([6]).

(6) Certificering af administrerede sikkerhedstjenester er ikke kun relevant for udvælgelsesprocessen til EU's cybersikkerhedsreserve oprettet ved forordning (EU) 2025/38, men også en vigtig kvalitetsindikator for private og offentlige enheder, der har til hensigt at købe sådanne tjenester. På grund af administrerede sikkerhedstjenesters kritiske karakter og følsomheden af de behandlede data, kan certificeringen tjene som vigtig vejledning og sikkerhed for mulige kunder med hensyn til disse tjenesters pålidelighed. Europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester har til formål at bidrage til at undgå fragmentering af det indre marked. Denne forordning har derfor til formål at forbedre det indre markeds funktion.

(7) Europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester bør føre til anvendelse af disse tjenester og til øget konkurrence mellem udbydere af administrerede sikkerhedstjenester. Uden at det berører målet om at sikre tilstrækkelige og passende niveauer af relevant teknisk viden og faglig integritet hos sådanne udbydere, bør sådanne certificeringsordninger derfor lette markedsadgangen og udbuddet af administrerede sikkerhedstjenester ved så vidt muligt at forenkle den potentielle reguleringsmæssige, administrative og finansielle byrde, som udbydere, navnlig små og mellemstore virksomheder (SMV'er), herunder mikrovirksomheder, kan støde på, når de tilbyder administrerede sikkerhedstjenester. For at tilskynde til udbredelsen af og stimulering af efterspørgslen på certificerede administrerede sikkerhedstjenester bør de europæiske cybersikkerhedscertificeringsordninger desuden bidrage til tilgængeligheden heraf, navnlig for mindre aktører såsom SMV'er, herunder mikrovirksomheder, 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.

(8) Det er vigtigt at yde støtte til SMV'er, herunder mikrovirksomheder, i forbindelse med gennemførelsen af denne forordning og med at rekruttere de specialiserede cybersikkerhedskompetencer og ekspertise, der er nødvendige for at levere administrerede sikkerhedstjenester i overensstemmelse med de krav, der er fastsat i denne forordning. Programmet for et digitalt Europa oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/694 ([7]) og andre relevante EU-programmer fastsætter, at Kommissionen yder finansiel og teknisk støtte, der sætter disse virksomheder i stand til at bidrage til væksten i Unionens økonomi og til at styrke det fælles cybersikkerhedsniveau i Unionen, herunder ved at strømline den finansielle støtte fra programmet for et digitalt Europa og andre relevante EU-programmer og ved at støtte SMV'er, herunder mikrovirksomheder.

(9) Den europæiske certificeringsordning for administrerede sikkerhedstjenester bør bidrage til at sikre tilgængeligheden af sikre tjenester af høj kvalitet, som garanterer en sikker digital omstilling, og til at nå de mål, der er fastsat i politikprogrammet for det digitale årti 2030 oprettet ved Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 ([8]), navnlig med hensyn til målet om, at 75 % af Unionens virksomheder skal begynde at anvende cloud computing-tjenester, big data og kunstig intelligens, at mere end 90 % af SMV'erne, herunder mikrovirksomheder,

([6]) Europa-Parlamentets og Rådets forordning (EU) 2025/38 af 19. december 2024 om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybertrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240 (EUT L 166 af 11.5.2021, s. 1).

([8]) Europa-Parlamentets og Rådets forordning (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030 (EUT L 323 af 19.12.2022, s. 4).

som minimum skal opnå et grundlæggende niveau af digital intensitet, og at centrale offentlige tjenester er tilgængelige online.

(10) 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 hos udbyderne af sådanne tjenester. 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 administrerede sikkerhedstjenester kan dækkes af særlige europæiske cybersikkerhedscertificeringsordninger, er det derfor nødvendigt at ændre forordning (EU) 2019/881. Der bør tages hensyn til resultaterne af og anbefalingerne i den evaluering og gennemgang der er omhandlet i forordning (EU) 2019/881.

(11) Med henblik på at fremme væksten af et pålideligt indre marked og samtidig skabe partnerskaber med ligesindede tredjelande, bør den certificeringsproces, der etableres inden for rammerne for den europæiske cybersikkerheds-certificering fastsat ved forordning (EU) 2019/881, gennemføres på en måde, der fremmer international anerkendelse og tilpasning til internationale standarder.

(12) Unionen står 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 med titlen »Opbygning af cybersikkerhedskomponenter skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed (»EU's akademi for cybersikkerhedskompetencer«)«. Uddannelsesressourcer og formelle uddannelsesformer varierer, og viden kan erhverves på forskellige måder: formelt, f.eks. gennem universiteter eller kurser, eller uformelt, f.eks. gennem jobtræning eller erhvervserfaring inden for det relevante område. For at lette fremkomsten af administrerede sikkerhedstjenester af høj kvalitet og for at få et bedre overblik over sammensætningen af Unionens arbejdsstyrke inden for cybersikkerhed er det vigtigt, at samarbejdet mellem medlemsstaterne, Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed oprettet ved forordning (EU) 2019/881 (ENISA) og interessenter, herunder fra 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 certificeringen af cybersikkerhedsfærdigheder, bl.a. gennem den europæiske ramme for cybersikkerhedskompetencer. Et sådant samarbejde vil også fremme 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. Det er vigtigt, at sådant samarbejde har til formål at tiltrække flere kvinder og piger på området og bidrager til at afhjælpe den kønsbestemte forskel inden for naturvidenskab, teknologi, ingeniørvirksomhed og matematik, og at den private sektor sigter mod at levere uddannelse på arbejdspladsen, der tackler de mest efterspurgte færdigheder, med inddragelse af den offentlige forvaltning og nystartede virksomheder samt SMV'er, herunder mikrovirksomheder. Det er også vigtigt, at udbydere og medlemsstater samarbejder og bidrager til indsamling af data om situationen og udviklingen på arbejdsmarkedet inden for cybersikkerhed.

(13) ENISA spiller en vigtig rolle i udarbejdelsen af forslag til europæiske certificeringsordninger. Kommissionen bør ved udarbejdelsen af forslaget til Unionens almindelige budget vurdere de nødvendige budgetmidler til ENISA's stillingsfortegnelse i overensstemmelse med proceduren i artikel 29 i forordning (EU) 2019/881.

(14) Denne forordning indeholder bestemmelser om målrettede ændringer af forordning (EU) 2019/881 for at muliggøre oprettelsen af cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester. I den forbindelse specificeres og præciseres visse bestemmelser i nævnte forordning vedrørende forberedelsen og funktionen af alle europæiske cybersikkerhedscertificeringsordninger med henblik på at sikre deres gennemsigtighed og åbenhed. Sidstnævnte ændringer, som er begrænset til specificering eller præcisering af forordning (EU) 2019/881, navnlig ændringerne vedrørende de oplysninger, ENISA skal forelægge ved fremsendelsen af et forslag til ordning, ad hoc-arbejdsgruppen oprettet for hvert forslag til ordning og oplysninger og høring vedrørende europæiske cybersikkerhedscertificeringsordninger, bør ikke på nogen måde foregribe den bredere evaluering og gennemgang af nævnte forordning, der kræves i henhold til nævnte forordnings artikel 67, navnlig evalueringen af virkningen, effektiviteten og produktiviteten af nævnte forordnings afsnit om rammebestemmelsen for cybersikkerhedscer-tificering. Denne evaluering og gennemgang vedrørende nævnte afsnit bør baseres på en bred høring af interessenter og en fuldstændig og grundig analyse af de involverede procedurer.

(15) Målet for denne forordning, nemlig at muliggøre oprettelsen af europæiske cybersikkerhedscertificeringsordninger for administrerede sikkerhedstjenester, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af dens omfang og virkninger bedre kan nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål.

(16) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([9]) og afgav en udtalelse den 10. januar 2024 —

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 og IKT-processer samt 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, der er fastsat på EU-plan, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af specifikke IKT-produkter, IKT-tjenester og IKT-processer eller administrerede sikkerhedstjenester

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

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

b) Følgende nummer indsættes:

»14a) »administreret sikkerhedstjeneste«: en tjeneste ydet til en tredjepart bestående i at udføre eller yde bistand til aktiviteter vedrørende styring af cybersikkerhedsrisici, såsom håndtering af hændelser, penetrationstest, sikkerhedsrevisioner og konsulentbistand, herunder ekspertrådgivning, vedrørende teknisk støtte«.

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

»20) »teknisk specifikation«: 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

([9]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

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

22) »selvvurdering af overensstemmelse«: en handling foretaget af en producent eller udbyder af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, der evaluerer, hvorvidt IKT-produkterne, IKT-tjenesterne, IKT-processerne eller de administrerede sikkerhedstjenester opfylder kravene i en specifik europæisk cybersikkerhedscertificeringsordning«.

3) Artikel 4, stk. 6, affattes således:

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

4) I artikel 8 foretages følgende ændringer:

a) I stk. 1 foretages følgende ændringer:

i) Indledningen 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:«.

ii) Litra b) affattes således:

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

b) Stk. 3 affattes således:

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

c) Stk. 5 affattes således:

»5. ENISA fremmer indførelse og udbredelse af europæiske og internationale standarder for risikostyring og for IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenester.«

5) Artikel 46 affattes således:

»*Artikel 46*

Europæisk ramme for cybersikkerhedscertificering

1. Den europæiske ramme for cybersikkerhedscertificering etableres for at forbedre betingelserne for det indre markeds funktion ved at øge cybersikkerhedsniveauet i Unionen og muliggøre en harmoniseret tilgang på EU-plan til europæiske cybersikkerhedscertificeringsordninger for at skabe et digitalt indre marked for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester.

2. Den europæiske ramme for cybersikkerhedscertificering definerer en mekanisme til fastlæggelse af europæiske cybersikkerhedscertificeringsordninger og 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 tilstrækkeligt og passende niveau af relevant teknisk viden og faglig integritet.«

6) I artikel 47 foretages følgende ændringer:

a) Stk. 2 affattes således:

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

b) I stk. 3 foretages følgende ændringer:

i) Indledningen affattes således:

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

ii) Litra a) affattes således:

»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«.

iii) Følgende litra indsættes:

»ca) den teknologiske udvikling og tilgængeligheden og udviklingen af internationale cybersikkerhedscertificeringsordninger og internationale standarder anvendt i industrien«.

7) I artikel 49 foretages følgende ændringer:

a) Stk. 1-4 affattes således:

»1. Efter anmodning fra Kommissionen i henhold til artikel 48 udarbejder ENISA et forslag til ordning, som opfylder de gældende krav i artikel 51, 51a, 52 og 54.

2. Efter anmodning fra ECCG i henhold til artikel 48, stk. 2, kan ENISA udarbejde et forslag til ordning, som opfylder de gældende krav i artikel 51, 51a, 52 og 54. Afviser ENISA en sådan anmodning, begrunder det afvisningen. Enhver afgørelse om afvisning af en sådan anmodning træffes af bestyrelsen.

3. Under udarbejdelsen af forslaget til ordning hører ENISA rettidigt alle relevante interessenter ved hjælp af en formel, åben, gennemsigtig og inklusiv høringsproces. Når ENISA fremsender forslaget til ordning til Kommissionen i henhold til stk. 6, giver det oplysninger om, på hvilken måde det har opfyldt nærværende stykke.

4. For hvert forslag til ordning nedsætter ENISA en ad hoc-arbejdsgruppe i overensstemmelse med artikel 20, stk. 4, med henblik på at stille specifik rådgivning og ekspertise til rådighed for ENISA. Disse ad hoc-arbejdsgrupper omfatter, hvor det er relevant, og uden at det berører de procedurer og skønsbeføjelser, der er fastsat i artikel 20, stk. 4, eksperter fra medlemsstaternes offentlige forvaltninger, Unionens institutioner, organer, kontorer og agenturer og den private sektor.«

b) Stk. 7 affattes således:

»7. Kommissionen kan på grundlag af det af ENISA udarbejdede forslag til ordning vedtage gennemførelsesretsakter vedrørende europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der opfylder de relevante krav i artikel 51, 51a, 52 og 54. Gennemførelsesretsakterne vedtages efter undersøgelsesproceduren i artikel 66, stk. 2.«

8) Følgende artikel indsættes:

»*Artikel 49a*

Oplysninger og høring vedrørende europæiske cybersikkerhedscertificeringsordninger

1. Kommissionen skal offentliggøre oplysninger om dens anmodning til ENISA om at udarbejde et forslag til ordning eller om gennemgang af en eksisterende europæisk cybersikkerhedscertificeringsordning som omhandlet i artikel 48.

2. Under ENISA's udarbejdelse af et forslag til ordning i henhold til artikel 49 kan Europa-Parlamentet, Rådet eller begge anmode Kommissionen i dens egenskab af formand for ECCG og ENISA om hvert kvartal at fremlægge relevante oplysninger om et forslag til ordning. Efter anmodning fra Europa-Parlamentet eller Rådet kan ENISA efter aftale med Kommissionen og med forbehold af artikel 27 stille relevante dele af udkastet til en ordning til rådighed for Europa-Parlamentet og Rådet på en måde, der svarer til det krævede fortrolighedsniveau, og, hvor det er relevant, på en begrænset måde.

3. For at styrke dialogen mellem EU-institutionerne og bidrage til en formel, åben, gennemsigtig og inklusiv høringsproces kan Europa-Parlamentet, Rådet eller begge opfordre Kommissionen og ENISA til at drøfte spørgsmål vedrørende funktionen af europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester, IKT-processer eller administrerede sikkerhedstjenester.

4. Kommissionen tager, hvor det er relevant, hensyn til elementer, der udspringer af de synspunkter, som Europa-Parlamentet og Rådet har givet udtryk for om de spørgsmål, der er omhandlet i denne artikels stk. 3, når den evaluerer denne forordning i henhold til artikel 67.«

9) 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:«.

10) 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 de administrerede sikkerhedstjenester har den nødvendige kompetence, ekspertise og erfaring, herunder at det personale, der har til opgave at levere disse tjenester, har et tilstrækkeligt og passende niveau af teknisk viden og kompetence på det specifikke område, tilstrækkelig og relevant erfaring og den højeste grad af faglig integritet

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

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

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

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

f) at der foretages og tilgængeliggøres registrering til vurdering de data, tjenester og funktioner, der er tilgået, anvendt eller på anden måde behandlet, på hvilket tidspunkt og af hvem

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

11) 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 undergå.«

c) Stk. 5, 6 og 7 affattes således:

»5. En europæisk cybersikkerhedsattest eller EU-overensstemmelseserklæring, der henviser til tillidsniveauet »grundlæggende«, skal give sikkerhed for, at de IKT-produkter, IKT-tjenester, IKT-processer eller 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 eller 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 eller 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.«

12) 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 eller 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, IKT-processernes eller de administrerede sikkerhedstjenesters overensstemmelse med ordningen til rådighed for den nationale cybersikkerhedscertificeringsmyndighed udpeget i henhold til 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.«

13) 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 g) affattes således:

»g) de specifikke evalueringskriterier og -metoder, der skal anvendes, herunder typen af evaluering, for at påvise, at de gældende sikkerhedsmål omhandlet i artikel 51 og 51a er nået«.

c) Litra j) affattes således:

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

d) Litra l) affattes således:

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

e) Litra o) affattes således:

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

f) 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«.

14) 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 medfør af artikel 49, formodes at overholde kravene i en sådan ordning.«

b) Stk. 3 ændres således:

i) Første afsnit affattes således:

»Kommissionen vurderer regelmæssigt effektiviteten og anvendelsen af de vedtagne europæiske cybersikkerhedscertificeringsordninger, og hvorvidt en bestemt europæisk cybersikkerhedscertificeringsordning skal gøres obligatorisk ved hjælp af relevant EU-ret for at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, IKT-tjenester, IKT-processer og fra den 4. februar 2025 for administrerede sikkerhedstjenester i Unionen og for at forbedre det indre markeds funktion. Den første sådanne vurdering skal foretages senest den 31. december 2023 og efterfølgende vurderinger mindst hvert andet år derefter. Kommissionen identificerer på grundlag af resultatet af disse vurderinger de IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester, der er omfattet af en eksisterende certificeringsordning, og som skal omfattes af en obligatorisk certificeringsordning.«

ii) I tredje afsnit foretages følgende ændringer:

— 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«.

— 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 specifikke interesser og behov hos SMV'er, herunder mikrovirksomheder«.

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 henhold til artikel 58 udpegede nationale cybersikkerhedscertificeringsmyndighed, hvis denne myndighed er det organ, der udsteder den europæiske cybersikkerhedsattest, eller for det i artikel 60 omhandlede overensstemmelsesvurderingsorgan.

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

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

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

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

16) 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 område, i samarbejde med andre relevante markedsovervågningsmyndigheder

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

ii) Litra h) affattes således:

»h) samarbejde med andre nationale cybersikkerhedscertificeringsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters, IKT-tjenesters, IKT-processers eller 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.«

17) 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)«.

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

»2. Evalueringen skal også vurdere virkningen og effektiviteten af bestemmelserne i afsnit III i denne forordning, herunder de procedurer, der fører til vedtagelse af europæiske cybersikkerhedscertificeringsordninger og deres database, med hensyn til målsætningerne om at sikre et tilstrækkeligt niveau for IKT-produkters, IKT-tjenesters, IKT-processers og administrerede sikkerhedstjenesters cybersikkerhed i Unionen og forbedre det indre markeds funktion.

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

19) Bilaget ændres som angivet i bilaget til nærværende forordning.

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 Bruxelles, den 19. december 2024.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	BÓKA J.
Formand	*Formand*

BILAG

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

1) Punkt 2-5 affattes således:

»2. Et overensstemmelsesvurderingsorgan skal være et tredjepartsorgan, der er uafhængigt af den organisation eller de IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, som det vurderer.

3. Et organ, der er medlem af en erhvervsorganisation og/eller brancheforening, som repræsenterer virksomheder, der er involveret i udformning, fremstilling, levering, sammenbygning, brug eller vedligeholdelse af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, som det vurderer, kan anses for at være et overensstemmelsesvurderingsorgan, forudsat at det er påvist, at det er uafhængigt, og at der ikke foreligger nogen interessekonflikt.

4. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for udførelsen af overensstemmelsesvurderingsopgaverne, må ikke være konstruktør, producent, leverandør, installatør, køber, ejer, bruger eller vedligeholder af det IKT-produkt, den IKT-tjeneste, den IKT-proces eller administrerede sikkerhedstjenester, der vurderes, eller repræsentere nogen af disse parter. Dette forbud udelukker ikke, at overensstemmelsesvurderingsorganet bruger de IKT-produkter, der er vurderet og nødvendige for, at det kan udføre sit arbejde, eller brug af sådanne IKT-produkter til personlige formål.

5. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsopgaverne, må ikke være direkte involveret i udformning, fremstilling eller konstruktion, levering, markedsføring, installation, anvendelse eller vedligeholdelse af de IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester, der vurderes, eller repræsentere parter, der er involveret i disse aktiviteter. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsopgaverne, må ikke deltage i aktiviteter, som kan være i strid med deres objektivitet og integritet i forbindelse med deres overensstemmelsesvurderingsaktiviteter. Dette forbud gælder navnlig rådgivningstjenester.«

2) I punkt 10 foretages følgende ændringer:

a) Indledningen affattes således:

»10. Et overensstemmelsesvurderingsorgan skal til enhver tid og for hver overensstemmelsesvurderingsprocedure og hver type, kategori eller underkategori af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester have følgende til rådighed i nødvendigt omfang:«.

b) Litra c) affattes således:

»c) procedurer, der sætter det i stand til at udføre sine aktiviteter under behørig hensyntagen til en virksomheds størrelse, den sektor, som den opererer inden for, og dens struktur, til graden af kompleksitet af teknologi for det pågældende IKT-produkt, den pågældende IKT-tjeneste, den pågældende IKT-proces eller for den pågældende administrerede sikkerhedstjeneste og til fremstillingsprocessens karakter af masse- eller serieproduktion.«

3) Punkt 19 og 20 affattes således:

»19. Overensstemmelsesvurderingsorganer skal opfylde kravene i den relevante harmoniserede standard som defineret i artikel 2, nr. 9), i forordning (EF) nr. 765/2008 med henblik på akkrediteringen af overensstemmelsesvurderingsorganer, der foretager certificeringen af IKT-produkter, IKT-tjenester, IKT-processer eller administrerede sikkerhedstjenester.

20. Overensstemmelsesvurderingsorganer skal sikre, at prøvningslaboratorier, der anvendes til overensstemmelsesvurdering, opfylder kravene i den relevante harmoniserede standard som defineret i artikel 2, nr. 9), i forordning (EF) nr. 765/2008 med henblik på akkrediteringen af laboratorier, der gennemfører prøvning.«

Der er fremsat en erklæring vedrørende denne retsakt, og den kan findes i EUT C, C/2025/307, 15.1.2025, og via følgende link: ELI: http://data.europa.eu/eli/C/2025/307/oj.