2025/37

15.1.2025

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2025/37

av den 19 december 2024

om ändring av förordning (EU) 2019/881 vad gäller utlokaliserade säkerhetstjänster

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) I Europaparlamentets och rådets förordning (EU) 2019/881 ([3]) fastställs ett ramverk för inrättandet av europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för produkter, tjänster och processer på området informations- och kommunikationsteknik (IKT) i unionen samt i syfte att undvika en fragmentering av den inre marknaden när det gäller ordningar för cybersäkerhetscertifiering i unionen.

(2) För att säkerställa unionens motståndskraft mot cyberattacker och för att förebygga sårbarheter på den inre marknaden är denna förordning avsedd att komplettera det övergripande regelverket med övergripande cybersäkerhetskrav för produkter med digitala element enligt Europaparlamentets och rådets förordning (EU) 2024/2847 ([4]), som föreskriver säkerhetsmålsättningar för utlokaliserade säkerhetstjänster, samt tillämpning och tillförlitlighet av de tjänsterna.

(3) Utlokaliserade säkerhetstjänster tillhandahålls av leverantörer av utlokaliserade säkerhetstjänster enligt definitionen i artikel 6.40 i Europaparlamentets och rådets direktiv (EU) 2022/2555 ([5]). Definitionen av utlokaliserade säkerhetstjänster i denna förordning bör därför överensstämma med den för utlokaliserade säkerhetstjänster i direktiv (EU) 2022/2555. De tjänsterna består i att utföra, eller tillhandahålla stöd för, verksamhet som rör deras kunders hantering av cybersäkerhetsrisker, och har blivit allt viktigare när det gäller att förhindra och mildra incidenter. Leverantörerna av dessa tjänster betraktas därför vara väsentliga eller viktiga entiteter som tillhör en högkritisk sektor enligt direktiv (EU) 2022/2555. Såsom anges i skäl 86 i det direktivet har leverantörer av utlokaliserade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Leverantörer av utlokaliserade säkerhetstjänster har dock också själva varit mål för cyberattacker och utgör en särskild risk, eftersom de är nära integrerade i sina kunders verksamhet. Det är därför viktigt att väsentliga och viktiga entiteter i den mening som avses i direktiv (EU) 2022/2555 visar större noggrannhet vid valet av leverantörer av utlokaliserade säkerhetstjänster.

([1]) EUT C 349, 29.9.2023, s. 167.
([2]) Europaparlamentets ståndpunkt av den 24 april 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den 2 december 2024.
([3]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).
([4]) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

(4) Definitionen av utlokaliserade säkerhetstjänster enligt denna förordning innehåller en icke uttömmande förteckning över utlokaliserade säkerhetstjänster som skulle kunna omfattas av europeiska ordningar för cybersäkerhetscertifiering, såsom hantering av incidenter, penetrationstestning, säkerhetsrevisioner och rådgivning för tekniskt stöd. Utlokaliserade säkerhetstjänster skulle kunna omfatta cybersäkerhetstjänster som stöder beredskap för, förebyggande, upptäckt, analys och begränsning av, hantering av och återhämtning från incidenter. Tillhandahållande av underrättelser om cyberhot och riskbedömning i samband med tekniskt stöd skulle också kunna klassificeras som utlokaliserade säkerhetstjänster. Det skulle kunna finnas separata europeiska ordningar för cybersäkerhetscertifiering för olika utlokaliserade säkerhetstjänster. De europeiska cybersäkerhetscertifikat som utfärdas i enlighet med sådana ordningar bör hänvisa till specifika utlokaliserade säkerhetstjänster hos en viss leverantör av de tjänsterna.

(5) Leverantörer av utlokaliserade säkerhetstjänster kan också spela en viktig roll när det gäller unionsåtgärder till stöd för hantering och initial återhämtning i händelse av betydande incidenter och storskaliga cybersäkerhetsincidenter, som är beroende av tjänster från betrodda privata leverantörer och testning av kritiska entiteter för potentiella sårbarheter på grundval av säkerhetsriskbedömningar på unionsnivå. Certifiering av utlokaliserade säkerhetstjänster skulle kunna spela en roll vid urvalet av betrodda leverantörer av utlokaliserade säkerhetstjänster enligt definitionen i Europaparlamentets och rådets förordning (EU) 2025/38 ([6]).

(6) Certifieringen av utlokaliserade säkerhetstjänster är inte endast relevant för förfarandet för urvalet till EU:s cybersäkerhetsreserv som inrättats genom förordning (EU) 2025/38, utan är även en viktig kvalitetsindikator för privata och offentliga entiteter som avser att köpa sådana tjänster. Mot bakgrund av utlokaliserade säkerhetstjänsters kritiska karaktär och känsligheten hos de data som behandlats skulle certifieringen kunna ge potentiella kunder viktig vägledning och visshet i fråga om de tjänsterna tillförlitlighet. Europeiska cybersäkerhetscertifieringsordningar för utlokaliserade säkerhetstjänster är tänkta att bidra till att undvika en fragmentering av den inre marknaden. Denna förordning syftar därför till att förbättra den inre marknadens funktion.

(7) Europeiska ordningar för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster bör leda till att dessa tjänster används och till ökad konkurrens mellan leverantörer som erbjuder utlokaliserade säkerhetstjänster. Utan att det påverkar målet att säkerställa tillräckliga och lämpliga nivåer av relevant teknisk kunskap och yrkesintegritet hos sådana leverantörer bör certifieringssystemen därför underlätta marknadstillträde och erbjudande av utlokaliserade säkerhetstjänster genom att i möjligaste mån förenkla den potentiella regelmässiga, administrativa och ekonomiska börda som leverantörer, särskilt små och medelstora företag, inbegripet mikroföretag, skulle kunna stöta på när de erbjuder utlokaliserade säkerhetstjänster. Dessutom bör europeiska ordningar för cybersäkerhetscertifiering uppmuntra användningen av och stimulera efterfrågan på utlokaliserade säkerhetstjänster genom att bidra till att göra dem tillgängliga, särskilt för mindre aktörer, såsom små och medelstora företag, inbegripet mikroföretag, samt lokala och regionala myndigheter med begränsad kapacitet och begränsade resurser, men som är mer benägna att drabbas av cybersäkerhetsöverträdelser med finansiella, rättsliga, anseendemässiga och operativa konsekvenser.

(8) Det är viktigt att ge stöd till mikroföretag och små och medelstora företag, inbegripet mikroföretag, vid genomförandet av denna förordning och vid rekryteringen av den specialiserade cybersäkerhetskompetens och sakkunskap som krävs för att tillhandahålla utlokaliserade säkerhetstjänster i enlighet med de krav som fastställs i denna förordning. I programmet för ett digitalt Europa inrättat genom Europaparlamentets och rådets förordning (EU) 2021/694 ([7]) och andra relevanta unionsprogram föreskrivs att kommissionen bör inrätta ekonomiskt och tekniskt stöd som gör det möjligt för dessa företag att bidra till tillväxt av unionens ekonomi och till att stärka den gemensamma cybersäkerhetsnivån i unionen, inbegripet genom att rationalisera det ekonomiska stödet från programmet för ett digitalt Europa och andra relevanta unionsprogram och genom att stödja små och medelstora företag, inbegripet mikroföretag.

(9) Europeiska ordningarna för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster bör bidra till tillgången på säkra tjänster av hög kvalitet som garanterar en säker digital omställning och till uppnåendet av de mål som fastställs i policyprogrammet för det digitala decenniet 2030 inrättat genom Europaparlamentets och rådets beslut (EU) 2022/2481 ([8]), särskilt när det gäller målet att 75 % av företagen i unionen ska börja använda molntjänster, stordata eller artificiell intelligens, att mer än 90 % av de små och medelstora företagen, inbegripet mikroföretag,

([6]) Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsakten) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 (EUT L 166, 11.5.2021, s. 1).

([8]) Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030 (EUT L 323, 19.12.2022, s. 4).

åtminstone ska uppnå en grundläggande nivå av digital intensitet och att viktiga offentliga tjänster ska vara tillgängliga online.

(10) Utöver de införda IKT-produkterna, IKT-tjänsterna eller IKT-processerna tillhandahålls genom de utlokaliserade säkerhetstjänsterna ofta ytterligare tjänstefunktioner som är beroende av kompetensen, sakkunskapen och erfarenheten hos personal vid leverantörer av sådana tjänster. En mycket hög nivå på den kompetensen, sakkunskapen och erfarenheten samt lämpliga interna förfaranden bör vara en del av säkerhetsmålsättningarna för att säkerställa en mycket hög kvalitet på de utlokaliserade säkerhetstjänster som tillhandahålls. För att säkerställa att alla aspekter av utlokaliserade säkerhetstjänster kan omfattas av särskilda europeiska ordningar för cybersäkerhetscertifiering är det därför nödvändigt att ändra förordning (EU) 2019/881. Resultaten och rekommendationerna från den utvärdering och översyn som föreskrivs i förordning (EU) 2019/881 bör beaktas.

(11) I syfte att underlätta tillväxten av en tillförlitlig inre marknad och samtidigt skapa partnerskap med likasinnade tredjeländer bör den certifieringsprocess som inrättas inom det europeiska ramverk för cybersäkerhetscertifiering som föreskrivs genom förordning (EU) 2019/881 genomföras på ett sätt som underlättar internationellt erkännande och anpassning till internationella standarder.

(12) Unionen står inför en kompetensbrist som kännetecknas av brist på kvalificerad arbetskraft och en snabbt föränderlig hotbild, vilket konstateras i kommissionens meddelande av den 18 april 2023 med titeln *Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens* (*EU-akademin för cyberkompetens*). Utbildningsresurser och formell utbildning skiljer sig åt, och kunskap kan förvärvas på olika sätt, formellt till exempel genom universitet eller kurser, eller icke-formellt, till exempel genom arbetsplatsanknuten utbildning eller praktik inom det relevanta området. För att underlätta framväxten av utlokaliserade säkerhetstjänster av hög kvalitet och få en bättre överblick över sammansättningen av unionens arbetskraft inom cybersäkerhet, är det viktigt att samarbetet mellan medlemsstaterna, kommissionen, Europeiska unionens cybersäkerhetsbyrå inrättad genom förordning (EU) 2019/881 (Enisa) och berörda parter, inbegripet den privata sektorn och den akademiska världen, stärks genom utveckling av offentlig-privata partnerskap, stöd till forsknings- och innovationsinitiativ, utveckling och ömsesidigt erkännande av gemensamma standarder och gemensam certifiering för cybersäkerhetskompetens, inbegripet genom den europeiska kompetensramen för cybersäkerhet. Ett sådant samarbete bör också underlätta rörligheten för yrkesverksamma inom cybersäkerhet i unionen samt integreringen av kunskap och utbildning om cybersäkerhet i utbildningsprogram, samtidigt som tillgång till lärlings- och praktikplatser säkerställs för ungdomar, inbegripet personer som bor i missgynnade regioner, såsom öar, glesbefolkade områden, landsbygdsområden och avlägsna områden. Det är viktigt att sådant samarbete syftar till att locka fler kvinnor och flickor till området och bidra till att överbrygga könsklyftan inom naturvetenskap, teknik, ingenjörsvetenskap och matematik, och att den privata sektorn strävar efter att tillhandahålla arbetsplatsanknuten utbildning som är inriktad på den mest efterfrågade kompetensen, med deltagande av offentlig förvaltning och uppstartsföretag samt små och medelstora företag, inbegripet mikroföretag. Det är också viktigt att leverantörerna och medlemsstaterna samarbetar och bidrar till insamlingen av uppgifter om situationen och utvecklingen på arbetsmarknaden för cybersäkerhet.

(13) Enisa spelar en viktig roll i utarbetandet av förslag till europeiska ordningar för cybersäkerhetscertifiering. Kommissionen bör bedöma nödvändiga budgetmedel för Enisas tjänsteförteckning, i enlighet med förfarandet som anges i artikel 29 i förordning (EU) 2019/881, vid utarbetandet av förslaget till unionens allmänna budget.

(14) I denna förordning föreskrivs riktade ändringar av förordning (EU) 2019/881 för att möjliggöra inrättandet av europeiska ordningar för cybersäkerhetscertifiering för leverantörer av utlokaliserade säkerhetstjänster. I samband med detta specificeras och förtydligas även vissa bestämmelser i den förordningen om utarbetandet och driften av alla europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa deras transparens och öppenhet. De senare ändringarna, som är begränsade till specificering eller förtydligande av förordning (EU) 2019/881, särskilt ändringarna rörande den information som Enisa ska tillhandahålla vid översändande av ett förslag till certifieringsordning, de tillfälliga arbetsgrupper som inrättas för varje förslag till certifieringsordning och information och samråd med hänsyn till europeiska ordningar för cybersäkerhetscertifiering, bör inte på något sätt föregripa den bredare utvärdering och översyn av den förordningen som krävs enligt artikel 67 i den förordningen, särskilt utvärderingen av effekterna, ändamålsenligheten och effektiviteten av den förordningens titel avseende ramverket för cybersäkerhetscertifiering. Utvärderingen och översynen av den titeln bör baseras på ett brett samråd med berörda parter och en fullständig och grundlig analys av de berörda förfarandena.

(15) Eftersom målet för denna förordning, nämligen att göra det möjligt att inrätta europeiska ordningar för cybersäkerhetscertifiering av utlokaliserade säkerhetstjänster, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(16) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([9]) och avgav ett yttrande den 10 januari 2024.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av förordning (EU) 2019/881

Förordning (EU) 2019/881 ska ändras på följande sätt:

1. I artikel 1.1 första stycket ska led b ersättas med följande:

”b) ett ramverk för inrättandet av europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster i unionen samt i syfte att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen.”

2. Artikel 2 ska ändras på följande sätt:

a) Leden 9, 10 och 11 ska ersättas med följande:

”9. *europeisk ordning för cybersäkerhetscertifiering*: en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering eller bedömning av överensstämmelse av särskilda IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster.

10. *nationell ordning för cybersäkerhetscertifiering*: en komplett uppsättning regler, tekniska krav, standarder och förfaranden som utvecklas och antas av en nationell offentlig myndighet och som tillämpas vid certifiering eller vid bedömning av överensstämmelse av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som omfattas av tillämpningsområdet för den ordningen.

11. *europeiskt cybersäkerhetscertifikat*: ett dokument, utfärdat av behörigt organ, som intygar att en viss IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst har utvärderats för kontroll av överensstämmelse med specifika säkerhetskrav som fastställs i en europeisk ordning för cybersäkerhetscertifiering.”

b) Följande led ska införas:

”14a. *utlokaliserad säkerhetstjänst*: en tjänst till en tredje part som består i att utföra, eller tillhandahålla stöd för, eller ge råd om verksamhet som rör hantering av cybersäkerhetsrisker, såsom incidenthantering, penetrationstester, säkerhetsrevisioner och rådgivning, inbegripet expertrådgivning, för tekniskt stöd.”

c) Leden 20, 21 och 22 ska ersättas med följande:

”20. *teknisk specifikation*: ett dokument som anger de tekniska krav som ska uppfyllas av, eller vilka förfaranden för bedömning av överensstämmelse som gäller för en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst.

([9]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

21. *assuransnivå*: förtroendegrund för att en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst uppfyller säkerhetskraven i en särskild europeisk ordning för cybersäkerhetscertifiering och anger på vilken nivå en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst har utvärderats, men som i sig inte mäter säkerheten i den berörda IKT-produkten, IKT-tjänsten, IKT-processen eller utlokaliserade säkerhetstjänsten.

22. *egenkontroll av överensstämmelse*: en åtgärd som genomförs av en tillverkare eller en leverantör av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, som utvärderar om dessa IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster uppfyller kraven i en särskild europeisk ordning för cybersäkerhetscertifiering.”

3. Artikel 4.6 ska ersättas med följande:

”6. Enisa ska främja användningen av europeisk cybersäkerhetscertifiering, i syfte att undvika en fragmentering av den inre marknaden. Enisa ska bidra till inrättandet och underhållandet av ett europeiskt ramverk för cybersäkerhetscertifiering i enlighet med avdelning III i denna förordning, i syfte att öka transparensen i fråga om cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster och därigenom stärka förtroendet för den digitala inre marknaden och dess konkurrenskraft.”

4. Artikel 8 ska ändras på följande sätt:

a) Punkt 1 ska ändras på följande sätt:

i) Inledningsfrasen ska ersättas med följande:

”1. Enisa ska stödja och främja utvecklingen och genomförandet av unionens politik för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster, enligt avdelning III i denna förordning, genom att”

ii) Led b ska ersättas med följande:

”b) utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordning*) för IKT-produkter och IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster i enlighet med artikel 49.”

b) Punkt 3 ska ersättas med följande:

”3. Enisa ska sammanställa och offentliggöra riktlinjer och utveckla god praxis, däribland om principer om it-hygien när det gäller cybersäkerhetskraven för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster, i samarbete med nationella myndigheter för cybersäkerhetscertifiering och branschen på ett formellt, standardiserat och transparent sätt.”

c) Punkt 5 ska ersättas med följande:

”5. Enisa ska underlätta upprättandet och tillämpningen av europeiska och internationella standarder för riskhantering och för säkerheten hos IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster.”

5. Artikel 46 ska ersättas med följande:

”*Artikel 46*

Europeiskt ramverk för cybersäkerhetscertifiering

1. Ett europeiskt ramverk för cybersäkerhetscertifiering ska inrättas för att förbättra förutsättningarna för den inre marknadens funktion genom att höja cybersäkerhetsnivån i unionen och möjliggöra en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering i syfte att skapa en digital inre marknad för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster.

2. Genom det europeiska ramverket för cybersäkerhetscertifiering ska en mekanism fastställas för inrättandet av europeiska ordningar för cybersäkerhetscertifiering och för att intyga att de IKT-produkter, IKT-tjänster och IKT-processer som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, tjänster och processer under hela

dess livscykel. Dessutom ska den intyga att utlokaliserade säkerhetstjänster som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos data som är föremål för åtkomst, behandling, lagring eller överföring i samband med tillhandahållandet av dessa tjänster, och att dessa tjänster tillhandahålls kontinuerligt med erforderlig kompetens, sakkunskap och erfarenhet av personal med tillräcklig och lämplig nivå av relevant teknisk kunskap och yrkesintegritet."

6. Artikel 47 ska ändras på följande sätt:

a) Punkt 2 ska ersättas med följande:

"2. I unionens löpande arbetsprogram ska det särskilt ingå en förteckning över IKT-produkter, IKT-tjänster och IKT-processer, och utlokaliserade säkerhetstjänster eller kategorier av sådana, som kan gagnas av att omfattas av en europeisk ordning för cybersäkerhetscertifiering."

b) Punkt 3 ska ersättas med följande:

i) Inledningsfrasen ska ersättas med följande:

"3. Inkludering i unionens löpande arbetsprogram av specifika IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, eller kategorier av sådana, ska motiveras av ett eller flera av följande skäl:"

ii) Led a ska ersättas med följande:

"a) Tillgänglighet och utveckling av nationella ordningar för cybersäkerhetscertifiering omfattande en specifik kategori av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster och i synnerhet med hänsyn till risken för fragmentering."

iii) Följande led ska införas:

"ca) Teknisk utveckling och tillgång till och utveckling av internationella ordningar för cybersäkerhetscertifiering och internationella standarder och standarder använda av industrin."

7. Artikel 49 ska ändras på följande sätt:

a) Punkterna 1–4 ska ersättas med följande:

"1. Efter en begäran från kommissionen enligt artikel 48 ska Enisa utarbeta ett förslag till certifieringsordning som uppfyller de tillämpliga kraven i artiklarna 51, 51a, 52 och 54.

2. Efter en begäran från europeiska gruppen för cybersäkerhetscertifiering enligt artikel 48.2 får Enisa utarbeta ett förslag till certifieringsordning som uppfyller de tillämpliga kraven i artiklarna 51, 51a, 52 och 54. Om Enisa avvisar en sådan begäran ska den ange skälen till avslaget. Beslut om att avvisa en sådan begäran ska fattas av styrelsen.

3. Vid utarbetandet av ett förslag till certifieringsordning ska Enisa i god tid samråda med alla berörda intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess. När Enisa översänder förslaget till certifieringsordning till kommissionen enligt punkt 6, ska Enisa lämna information om på vilket sätt den har följt denna punkt.

4. För varje förslag till certifieringsordning ska Enisa inrätta en tillfällig arbetsgrupp i enlighet med artikel 20.4 i syfte att tillhandahålla Enisa särskild rådgivning och sakkunskap. Dessa tillfälliga arbetsgrupper ska, när så är lämpligt och utan att det påverkar de förfaranden och den skönsmässiga bedömning som föreskrivs i artikel 20.4, inbegripa experter från medlemsstaternas offentliga förvaltningar, unionens institutioner, organ och byråer samt den privata sektorn."

b) Punkt 7 ska ersättas med följande:

"7. På grundval av förslaget till certifieringsordning som Enisa lagt fram, får kommissionen anta genomförandeakter för europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som uppfyller de relevanta kraven i artiklarna 51, 51a, 52 och 54. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2."

8. Följande artikel ska införas:

”*Artikel 49a*

Information och samråd om europeiska ordningar för cybersäkerhetscertifiering

1. Kommissionen ska offentliggöra informationen om sin begäran till Enisa att utarbeta ett förslag till certifieringsordning eller att se över en befintlig europeisk ordning för cybersäkerhetscertifiering som avses i artikel 48.

2. Under Enisas utarbetande av ett förslag till certifieringsordning enligt artikel 49 får Europaparlamentet, rådet eller båda begära att kommissionen i egenskap av ordförande för den europeiska gruppen för cybersäkerhetscertifiering och Enisa varje kvartal lägger fram relevant information om ett utkast till ett förslag till certifieringsordning. På begäran av Europaparlamentet eller rådet får Enisa, i samförstånd med kommissionen och utan att det påverkar tillämpningen av artikel 27, göra relevanta delar av ett förslag till certifieringsordning tillgängliga för Europaparlamentet och rådet på ett sätt som är lämpligt med hänsyn till den konfidentialitetsnivå som krävs, och när så är lämpligt på ett begränsat sätt.

3. För att stärka dialogen mellan unionens institutioner och bidra till en formell, öppen, transparent och inkluderande samrådsprocess får Europaparlamentet, rådet eller båda uppmana kommissionen och Enisa att diskutera frågor som rör hur europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster fungerar.

4. Kommissionen ska, när så är lämpligt, beakta alla aspekter av de synpunkter som framförts av Europaparlamentet och av rådet om de frågor som avses i punkt 3 i denna artikel när den utvärderar denna förordning enligt artikel 67.”

9. Artikel 51 ska ändras på följande sätt:

a) Rubriken ska ersättas med följande:

”Säkerhetsmålsättningarna för europeiska ordningar för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster och IKT-processer”.

b) Inledningsfrasen ska ersättas med följande:

”En europeisk ordning för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster eller IKT-processer ska vara utformad för att, i tillämpliga fall, uppnå åtminstone följande säkerhetsmålsättningar:”.

10. Följande artikel ska införas:

”*Artikel 51a*

Säkerhetsmålsättningarna för europeiska ordningar för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster

En europeisk ordning för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster ska vara utformad för att, i tillämpliga fall, uppnå åtminstone följande säkerhetsmålsättningar:

a) Att de utlokaliserade säkerhetstjänsterna förses med den kompetens, sakkunskap och erfarenhet som krävs, inbegripet att den personal som fått uppgiften att tillhandahålla dessa tjänster har en tillräcklig och lämplig nivå av teknisk kunskap och kompetens på det specifika området, tillräcklig och lämplig erfarenhet och största möjliga yrkesintegritet.

b) Att leverantören har lämpliga interna förfaranden för att säkerställa att de utlokaliserade säkerhetstjänsterna alltid tillhandahålls med en tillräcklig och lämplig kvalitetsnivå.

c) Att skydda data som är föremål för åtkomst, behandling, lagring eller överföring i samband med tillhandahållandet av utlokaliserade säkerhetstjänster mot åtkomst, lagring, utlämnande, förstöring eller annan behandling, som sker oavsiktligt eller otillåtet, eller förlust eller ändring eller brist på tillgänglighet.

d) Att säkerställa att tillgängligheten och tillgången avseende data, tjänster och funktioner återställs i god tid vid en fysisk eller teknisk incident.

e) Att behöriga personer, program eller maskiner kan få åtkomst endast till de data, tjänster eller funktioner som omfattas av deras åtkomsträttigheter.

f) Att registret bevaras och är tillgängligt för bedömning av vilka data, tjänster eller funktioner som någon haft åtkomst till, som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem.

g) Att de IKT-produkter, IKT-tjänster och IKT-processer som används vid tillhandahållandet av de utlokaliserade säkerhetstjänsterna är säkra genom sin konstruktion och i sitt grundutförande, och, i tillämpliga fall, inbegriper de senaste säkerhetsuppdateringarna och inte innehåller några kända sårbarheter.”

11. Artikel 52 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. En europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster: ’grundläggande’, ’betydande’ eller ’hög’. Assuransnivån ska stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst, i form av sannolikhet för och inverkan av en eventuell incident.”

b) Punkt 3 ska ersättas med följande:

”3. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering, inbegripet motsvarande säkerhetsfunktioner och motsvarande stringens och djup i fråga om den utvärdering som IKT-produkten, IKT-tjänsten, IKT-processen eller den utlokaliserade säkerhetstjänsten ska genomgå.”

c) Punkterna 5, 6 och 7 ska ersättas med följande:

”5. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ’grundläggande’ ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för vilka det certifikatet eller den EU-försäkran om överensstämmelse har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera kända grundläggande risker för incidenter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen. Om en sådan granskning inte är lämplig ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

6. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ’betydande’ ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för vilka det certifikatet har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera kända cyberrisker, och risken för incidenter och cyberattacker som genomförs av aktörer med begränsade kunskaper och resurser. Den utvärdering som ska göras ska innefatta åtminstone följande: en granskning för att visa att allmänt kända sårbarheter inte föreligger och testning för att visa att IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner. Om sådana utvärderingar inte är lämpliga ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

7. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ’hög’ ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för vilka det certifikatet har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera risken för avancerade cyberattacker som genomförs av aktörer med omfattande kunskaper och resurser. Den utvärdering som ska göras ska innefatta åtminstone följande: en granskning för att visa att allmänt kända sårbarheter inte föreligger, testning för att visa att IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner, med den senaste tekniken, och en bedömning av motståndskraften mot kunniga angripare genom penetrationsprovning. Om sådana utvärderingar inte är lämpliga får alternativa insatser utföras.”

12. Artikel 53.1, 53.2 och 53.3 ska ersättas med följande:

”1. En europeisk ordning för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster möjlighet att göra en självbedömning av överensstämmelse. En självbedömning av överensstämmelse ska endast tillåtas i förhållande till IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster med låg risk som motsvarar assuransnivån ’grundläggande’.

2. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster får utfärda en EU-försäkran om överensstämmelse med angivande av att det har visats att kraven i ordningen är uppfyllda. Genom att upprätta en sådan försäkran tar tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster ansvar för att IKT-produkten, IKT-tjänsten, IKT-processen eller den utlokaliserade säkerhetstjänsten överensstämmer med de krav som anges i den ordningen.

3. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster ska, under en period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering, ge den nationella myndighet för cybersäkerhetscertifiering som utsetts enligt artikel 58 tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas, IKT-tjänsternas eller de utlokaliserade säkerhetstjänsternas överensstämmelse med ordningen. En kopia av EU-försäkran om överensstämmelse ska lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.”

13. Artikel 54.1 ska ändras på följande sätt:

a) Led a ska ersättas med följande:

”a) Föremålet och tillämpningsområdet för certifieringsordningen, inbegripet typen eller kategorierna av de IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som omfattas av certifieringsordningen.”

b) Led g ska ersättas med följande:

”g) De särskilda bedömningskriterier och -metoder som används, inklusive utvärderingstyper, i syfte att visa att de tillämpliga säkerhetsmålsättningar som avses i artikel 51 och 51a uppnås.”

c) Led j ska ersättas med följande:

”j) Reglerna för övervakning av efterlevnaden av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster vad gäller kraven i europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven.”

d) Led l ska ersättas med följande:

”l) Regler om följderna för IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som har certifierats eller för vilka en EU-försäkran om överensstämmelse har utfärdats, men som inte överensstämmer med kraven i ordningen.”

e) Led o ska ersättas med följande:

”o) Identifiering av nationella eller internationella ordningar för cybersäkerhetscertifiering som omfattar samma typ eller kategorier av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, säkerhetskrav, utvärderingskriterier och utvärderingsmetoder samt assuransnivåer.”

f) Led q ska ersättas med följande:

”q) Den period under vilken tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster ska hålla tillgänglig EU-försäkran om överensstämmelse, den tekniska dokumentationen och all annan relevant information som ska göras tillgänglig.”

14. Artikel 56 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som har certifierats enligt en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 ska förutsättas överensstämma med kraven i en sådan ordning.”

b) Punkt 3 ska ändras på följande sätt:

i) Första stycket ska ersättas med följande:

”Kommissionen ska regelbundet bedöma effektiviteten hos och användningen av de antagna europeiska ordningarna för cybersäkerhetscertifiering och huruvida en specifik europeisk ordning för cybersäkerhetscertifiering ska göras obligatoriskt genom unionsrätten i syfte att säkerställa en adekvat cybersäkerhetsnivå för IKT-produkter, IKT-tjänster, IKT-processer och från och med 4 februari 2025 utlokaliserade säkerhetstjänster i unionen och förbättra den inre marknadens funktion. Den första bedömningen ska göras senast den 31 december 2023, och efterföljande bedömningar ska göras minst en gång vartannat år därefter. Kommissionen ska på grundval av resultatet av bedömningen fastställa vilka IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som ska omfattas av en existerande certifieringsordning som ska täckas av en obligatorisk certifieringsordning.”

ii) Tredje stycket ska ändras på följande sätt:

— Led a ska ersättas med följande:

”a) beakta åtgärdernas konsekvenser i kostnadsavseende för tillverkarna eller leverantörerna av de berörda IKT-produkterna, IKT-tjänsterna, IKT-processerna eller utlokaliserade säkerhetstjänsterna och för användarna samt de samhälleliga eller ekonomiska vinsterna med den förväntade höjningen av säkerhetsnivån för de berörda IKT-produkterna, IKT-tjänsterna, IKT-processerna eller utlokaliserade säkerhetstjänsterna,”.

— Led d ska ersättas med följande:

”d) beakta eventuella genomförandefrister och övergångsåtgärder och övergångsperioder, i synnerhet åtgärdens tänkbara inverkan på tillverkare eller leverantörer av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, inbegripet särskilda intressen och behov för små och medelstora företag, inbegripet mikroföretag.”

c) Punkterna 7 och 8 ska ersättas med följande:

”7. Den fysiska eller juridiska person som lämnar in sina IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för certifiering ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndighet för cybersäkerhetscertifiering som utses enligt artikel 58, om denna myndighet är det organ som utfärdar det europeiska cybersäkerhetscertifikatet, eller för det organ för bedömning av överensstämmelse som avses i artikel 60.

8. Innehavaren av ett europeiskt cybersäkerhetscertifikat ska informera den myndighet eller det organ som avses i punkt 7 om alla sårbarheter eller oriktigheter som upptäcks senare och som rör säkerheten för den certifierade IKT-produkten, IKT-tjänsten, IKT-processen eller utlokaliserade säkerhetstjänsten som kan påverka överensstämmelsen med de krav som sammanhänger med certifieringen. Den myndigheten eller det organet ska utan onödigt dröjsmål vidarebefordra denna information till den berörda nationella myndigheten för cybersäkerhetscertifiering.”

15. Artikel 57.1 och 57.2 ska ersättas med följande:

”1. Utan att det påverkar tillämpningen av punkt 3 i denna artikel ska de nationella ordningarna för cybersäkerhetscertifiering och därtill hörande förfaranden, för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som omfattas av en europeisk ordning för cybersäkerhetscertifiering, upphöra att ha verkan från och med den dag som anges i den genomförandeakt som antagits enligt artikel 49.7. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som inte omfattas av en europeisk ordning för cybersäkerhetscertifiering ska kvarstå.

2. Medlemsstaterna ska inte införa nya nationella ordningar för cybersäkerhetscertifiering av de IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som redan omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.”

16. Artikel 58 ska ändras på följande sätt:

a) Punkt 7 ska ändras på följande sätt:

i) Leden a och b ska ersättas med följande:

”a) övervaka och kontrollera efterlevnaden av reglerna i europeiska ordningar för cybersäkerhetscertifiering enligt artikel 54.1 j för övervakning av IKT-produkters, IKT-tjänsters, IKT-processers och utlokaliserade säkerhetstjänsters överensstämmelse med kraven i de europeiska cybersäkerhetscertifikat som utfärdats inom deras respektive territorier, i samarbete med andra berörda marknadsövervakningsmyndigheter,

b) kontrollera att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som är etablerade inom deras respektive territorier fullgör och verkställer sina skyldigheter och att de genomför självbedömning av överensstämmelse, särskilt fullgörandet och verkställandet av dessa tillverkares och leverantörers skyldigheter som anges i artikel 53.2 och 53.3 och i motsvarande europeisk ordning för cybersäkerhetscertifiering.”

ii) Led h ska ersättas med följande:

”h) samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, inbegripet genom att utbyta information om IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som eventuellt avviker från kraven i denna förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och”.

b) Punkt 9 ska ersättas med följande:

”9. Nationella myndigheter för cybersäkerhetscertifiering ska samarbeta med varandra och med kommissionen, i synnerhet, genom att utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster.”

17. I artikel 59.3 ska leden b och c ersättas med följande:

”b) av förfarandena för övervakning och kontroll av efterlevnaden av reglerna om IKT-produkters, IKT-tjänsters, IKT-processers och utlokaliserade säkerhetstjänsters överensstämmelse med europeiska cybersäkerhetscertifikat enligt artikel 58.7 a,

c) av förfarandena för övervakning och verkställande av de skyldigheter som tillverkare eller tillhandahållare av IKT-produkter, IKT tjänster, IKT-processer eller utlokaliserade säkerhetstjänster har enligt artikel 58.7 b,”.

18. Artikel 67.2 och 67.3 ska ersättas med följande:

”2. Utvärderingen ska även bedöma effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i denna förordning, inbegripet de förfaranden som leder till antagandet av europeiska ordningar för cybersäkerhetscertifiering och deras evidensbas, i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster i unionen och förbättra den inre marknadens funktion.

3. I utvärderingen ska det bedömas om tillträde till den inre marknaden ska förutsätta att väsentliga cybersäkerhetskrav uppfyllts, för att förhindra att IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster som inte uppfyller de grundläggande cybersäkerhetskraven kommer in på den inre marknaden.”

19. Bilagan ska ändras i enlighet med bilagan till denna förordning.

Artikel 2

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 19 december 2024.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	BÓKA J.
Ordförande	*Ordförande*

BILAGA

Bilaga till förordning (EU) 2019/881 ska ändras på följande sätt:

1. Punkterna 2–5 ska ersättas med följande:

”2. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller de IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som det bedömer.

3. Ett organ som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i utformning, tillverkning, leverans, installation, användning eller underhåll av de IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som det bedömer, får anses vara ett organ för bedömning av överensstämmelse, förutsatt att det kan styrkas att det är oberoende och att inga intressekonflikter föreligger.

4. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för att utföra bedömningen av överensstämmelse, får inte utgöras av den som utformar, tillverkar, levererar, installerar, köper, äger, använder eller underhåller den IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst som bedöms, eller de som företräder någon av dessa parter. Det förbudet ska inte hindra att bedömda IKT-produkter som är nödvändiga för verksamheten inom organet för bedömning av överensstämmelse används eller att IKT-produkterna används för personligt bruk.

5. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får varken delta direkt i utformningen, tillverkningen eller konstruktionen, leveransen, marknadsföringen, installationen, användningen eller underhållet av dessa IKT-produkter, IKT-tjänster eller IKT-processer eller utlokaliserade säkerhetstjänster som bedöms, eller företräda de parter som bedriver denna verksamhet. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömningen av överensstämmelse. Det förbudet ska framför allt gälla konsulttjänster.”

2. Punkt 10 ska ändras på följande sätt:

a) Introduktionsfrasen ska ersättas med följande

”10. Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ, kategori eller underkategori av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, ska ett organ för bedömning av överensstämmelse ha till sitt förfogande”.

b) Led c ska ersättas med följande:

”c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda IKT-produktteknikens, IKT-tjänsteteknikens, IKT-processteknikens eller de berörda utlokaliserade säkerhetstjänsternas komplexitet och om det rör sig om massproduktion eller serietillverkning.”

3. Punkterna 19 och 20 ska ersättas med följande:

”19. Organen för bedömning av överensstämmelse ska uppfylla de krav som anges i relevant harmoniserad standard enligt definitionen i artikel 2.9 i förordning (EG) nr 765/2008 för ackreditering av organ för bedömning av överensstämmelse som utför certifiering av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster.

20. Organen för bedömning av överensstämmelse ska säkerställa att de provningslaboratorier som används för att prova överensstämmelsen uppfyller de krav som anges i relevant harmoniserad standard enligt definitionen i artikel 2.9 i förordning (EG) nr 765/2008 för ackreditering av laboratorier som utför provningar.”

Ett uttalande har gjorts med avseende på denna förordning och återfinns i EUT C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.