Europeiska unionens råd

Bryssel den 21 april 2023
(OR. en)

8511/23

Interinstitutionellt ärende:
2023/0108(COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	19 april 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 208 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om ändring av förordning (EU) 2019/881 vad gäller hanterade säkerhetstjänster

För delegationerna bifogas dokument – COM(2023) 208 final.

Bilaga: COM(2023) 208 final

EUROPEISKA
KOMMISSIONEN

Strasbourg den 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

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

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Denna motivering åtföljer förslaget till Europaparlamentets och rådets förordning om ändring av förordning (EU) 2019/881[1] vad gäller hanterade säkerhetstjänster.

Syftet med den föreslagna riktade ändringen är att göra det möjligt att, genom genomförandeakter från kommissionen, anta europeiska ordningar för cybersäkerhetscertifiering för ”hanterade säkerhetstjänster”, utöver IKT-produkter (informations- och kommunikationsteknikprodukter), IKT-tjänster och IKT-processer, som redan omfattas av cybersäkerhetsakten. Hanterade säkerhetstjänster spelar en allt viktigare roll för att förhindra och mildra cybersäkerhetsincidenter.

Rådet uppmanade i sina slutsatser av den 23 maj 2022[2] om utvecklingen av Europeiska unionens arbete på cyberområdet unionen och dess medlemsstater att öka ansträngningarna för att höja den övergripande cybersäkerhetsnivån, till exempel genom att underlätta nyetablering av tillförlitliga leverantörer av cybersäkerhetstjänster, och betonade att främjande av framväxten av sådana leverantörer bör vara en prioritering för EU:s industripolitik på cybersäkerhetsområdet. Det uppmanade också kommissionen att lägga fram olika alternativ för att främja framväxten av en tillförlitlig bransch för cybersäkerhetstjänster. Certifiering av hanterade säkerhetstjänster är ett effektivt sätt att bygga upp tilliten till dessa tjänsters kvalitet och därigenom underlätta framväxten av en tillförlitlig europeisk sektor för cybersäkerhetstjänster.

I det gemensamma meddelandet *EU:s politik för cyberförsvar*, som antogs av kommissionen och den höga representanten den 10 november 2022[3], angavs att kommissionen skulle undersöka möjligheten att utveckla ordningar för cybersäkerhetscertifiering på EU-nivå för cybersäkerhetsbranschen och privata företag. Leverantörerna av hanterade säkerhetstjänster kommer också att spela en viktig roll i cybersäkerhetsreserven på EU-nivå, vars gradvisa inrättande stöds av förslaget till cybersolidaritetslag, som läggs fram parallellt med denna förordning. Cybersäkerhetsreserven på EU-nivå ska användas för att stödja insatser samt åtgärder för omedelbar återhämtning i händelse av betydande och storskaliga cybersäkerhetsincidenter. De relevanta cybersäkerhetstjänsterna som tillhandahålls av ”betrodda leverantörer” som avses i cybersolidaritetslagen motsvarar ”hanterade säkerhetstjänster” i detta förslag.

Vissa medlemsstater har redan börjat anta certifieringsordningar för hanterade säkerhetstjänster. Det finns därför en växande risk för att den inre marknaden för hanterade säkerhetstjänster fragmenteras på grund av skillnader i cybersäkerhetscertifieringsordningarna inom unionen. Detta förslag gör det möjligt att inrätta EU-ordningar för cybersäkerhetscertifiering för dessa tjänster för att förhindra en sådan fragmentering.

---

1 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.

2 9364-2.

3 JOIN(2022) 49 final.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag är förenligt med cybersäkerhetsakten, som den ändrar. Det bygger på bestämmelserna i den akten och anpassar dem så att de även omfattar hanterade säkerhetstjänster. De föreslagna ändringarna är begränsade till vad som är absolut nödvändigt och ändrar inte cybersäkerhetsaktens egenskaper eller funktion.

Detta förslag är också förenligt med 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)[4]. Leverantörer av hanterade säkerhetstjänster betraktas som väsentliga eller viktiga entiteter som tillhör en högkritisk sektor i enlighet med direktiv (EU) 2022/2555. Enligt skäl 86 i det direktivet har leverantörer av hanterade 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 hanterade säkerhetstjänster har dock också själva varit mål för cyberattacker och utgör en särskild risk, eftersom de är nära integrerade i sina kunders verksamhet. Väsentliga och viktiga entiteter i den mening som avses i direktiv (EU) 2022/2555 bör därför visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster.

Detta förslag syftar till att förbättra kvaliteten på hanterade säkerhetstjänster och öka deras jämförbarhet. Det gör det därmed möjligt för väsentliga och viktiga entiteter att visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster, såsom föreskrivs i direktiv (EU) 2022/2555. Dessutom är definitionen av ”hanterade säkerhetstjänster” i detta förslag härledd från och ligger mycket nära definitionen av ”leverantörer av hanterade säkerhetstjänster” i direktiv (EU) 2022/2555. Av dessa skäl kompletterar förslaget och NIS 2-direktivet varandra i hög grad.

Slutligen kompletterar detta förslag och den föreslagna cybersolidaritetsakten varandra. I förslaget till cybersolidaritsakt fastställs ett förfarande för att välja ut leverantörer som ska bilda en cybersäkerhetsreserv på EU-nivå, vid vilket det bland annat bör tas hänsyn till huruvida de leverantörerna har erhållit en europeisk eller nationell cybersäkerhetscertifiering.. Framtida certifieringsordningar för hanterade säkerhetstjänster kommer därför att spela en viktig roll i genomförandet av cybersolidaritetsakten.

- **Förenlighet med unionens politik inom andra områden**

Detta förslag påverkar inte cybersäkerhetsaktens förenlighet med förordning (EU) 2016/679 (allmänna dataskyddsförordningen)[5] och dess bestämmelser om inrättande av certifieringsmekanismer samt sigill och märkningar för dataskydd i syfte att visa att personuppgiftsansvarigas och personuppgiftsbiträdens uppgiftsbehandling är förenlig med denna förordning. Cybersäkerhetsakten påverkar inte certifieringen av uppgiftsbehandling, inte heller om denna verksamhet ingår i produkter och tjänster, enligt den allmänna dataskyddsförordningen.

Detta förslag påverkar heller inte cybersäkerhetsaktens förenlighet med förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll[6], särskilt när det gäller ramen för nationella ackrediteringsorgan och organ för bedömning av överensstämmelse samt nationella tillsynsmyndigheter för certifiering.

---

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

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Genom detta förslag ändras cybersäkerhetsakten, som grundar sig på artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Liksom i fallet med cybersäkerhetsakten syftar detta förslag till att undvika fragmentering av den inre marknaden, nämligen genom att möjliggöra antagandet av europeiska ordningar för cybersäkerhetscertifiering för hanterade säkerhetstjänster. Medlemsstaterna har börjat anta nationella certifieringsordningar för hanterade säkerhetstjänster. Det finns därför en konkret risk för fragmentering av den inre marknaden i fråga om dessa tjänster, vilket detta förslag syftar till att åtgärda. Därför är artikel 114 i EUF-fördraget relevant rättslig grund för detta initiativ.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Målet att möjliggöra antagandet av europeiska ordningar för cybersäkerhetscertifiering för hanterad säkerhet och undvika en fragmentering av den inre marknaden kan inte uppnås på nationell nivå, utan endast på unionsnivå. Hanterade säkerhetstjänster, som den föreslagna ändringen särskilt inriktar sig på, erbjuds dessutom av leverantörer vars verksamhet omfattar hela unionen, i likhet med deras största potentiella kunders verksamhet. Åtgärder på unionsnivå är därför både nödvändiga och effektivare än åtgärder på nationell nivå.

- **Proportionalitet**

Förslaget är en riktad ändring av cybersäkerhetsakten. Det är begränsat till vad som är absolut nödvändigt för att uppnå dess mål, nämligen att möjliggöra antagandet av europeiska ordningar för cybersäkerhetscertifiering för hanterade säkerhetstjänster, utöver IKT-produkter, IKT-tjänster och IKT-processer. De föreslagna ändringarna anpassar i synnerhet tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering till att även omfatta ”hanterade säkerhetstjänster”, inför en definition av dessa tjänster som överensstämmer med NIS 2-direktivet, och ändrar säkerhetsmålsättningarna för den europeiska cybersäkerhetscertifieringen så att den anpassas till ”hanterade säkerhetstjänster”. De övriga ändringarna är av teknisk natur och syftar till att säkerställa att de relevanta artiklarna även gäller ”hanterade säkerhetstjänster”. Det föreslagna initiativet står därmed i proportion till målet.

- **Val av instrument**

Det lämpliga rättsliga instrumentet är en förordning, eftersom rättsakten ändrar förordning (EU) 2019/881.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Ej tillämpligt.

- **Samråd med berörda parter**

Riktade samråd med medlemsstaterna och Enisa har genomförts. I dessa samråd beskrev medlemsstaterna sin nuvarande verksamhet och sina synpunkter när det gäller certifiering av hanterade säkerhetstjänster. Enisa redogjorde för sina synpunkter och slutsatser från

diskussionerna med medlemsstaterna och berörda parter. De synpunkter och den information som mottagits från medlemsstaterna och Enisa har beaktats i detta förslag.

- **Insamling och användning av sakkunnigutlåtanden**

Ej tillämpligt.

- **Konsekvensbedömning**

Ett undantag från kravet på en konsekvensbedömning har begärts, eftersom förslaget är en mycket begränsad och riktad ändring av cybersäkerhetsakten. Det skulle ge kommissionen befogenhet att genom genomförandeakter anta certifieringsordningar för ”hanterade säkerhetstjänster”, utöver IKT-produkter, IKT-tjänster och IKT-processer, som redan omfattas av akten. Ändringen skulle dock inte få någon effekt förrän sådana certifieringsordningar har antagits i ett senare skede. Dessutom skulle ändringen inte ändra certifieringsordningarnas frivilliga karaktär.

- **Lagstiftningens ändamålsenlighet och förenkling**

Ej tillämpligt.

- **Grundläggande rättigheter**

Förslaget har inga konsekvenser för skyddet av de grundläggande rättigheterna.

4. BUDGETKONSEKVENSER

Ingen.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

De bestämmelser som ska ändras genom förslaget kommer att utvärderas som en del av den regelbundna utvärdering av cybersäkerhetsakten som kommissionen ska genomföra i enlighet med artikel 67 i den akten. I utvärderingen ska även en bedömning göras av effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i denna förordning i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer i unionen och förbättra den inre marknadens funktion. Förslaget innehåller en ändring som säkerställer att utvärderingen även omfattar hanterade säkerhetstjänster. Kommissionen översänder också en rapport om utvärderingen och sina slutsatser till Europaparlamentet, rådet och Enisas styrelse och offentliggör resultaten av rapporten.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Förslaget innehåller två artiklar. Artikel 1 innehåller ändringarna av förordning (EU) 2019/881, medan artikel 2 rör ikraftträdandet. Artikel 1 innehåller riktade ändringar för att ändra tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering i cybersäkerhetsakten så att det även omfattar ”hanterade säkerhetstjänster” (artiklarna 1 och 46 i cybersäkerhetsakten). Genom förslaget införs en definition av dessa tjänster, som är nära anpassad till definitionen av ”leverantörer av hanterade säkerhetstjänster” i NIS 2-direktivet (artikel 2 i cybersäkerhetsakten). Det läggs också till en ny artikel 51a om

säkerhetsmålsättningarna för europeisk cybersäkerhetscertifiering anpassad till ”hanterade säkerhetstjänster”. Slutligen innehåller förslaget ett antal tekniska ändringar för att säkerställa att de relevanta artiklarna även gäller ”hanterade säkerhetstjänster”.

2023/0108 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om ändring av förordning (EU) 2019/881 vad gäller hanterade 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,

med beaktande av Regionkommitténs yttrande,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I Europaparlamentets och rådets förordning (EU) 2019/881[7] fastställs 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 och IKT-processer i unionen samt i syfte att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen.

(2) Hanterade säkerhetstjänster, som är tjänster som består i att utföra, eller tillhandahålla stöd för, verksamhet som rör deras kunders hantering av cybersäkerhetsrisker, har blivit allt viktigare när det gäller att förhindra och mildra cybersäkerhetsincidenter. Leverantörerna av dessa tjänster betraktas därför som väsentliga eller viktiga entiteter som tillhör en högkritisk sektor i enlighet med Europaparlamentets och rådets direktiv (EU) 2022/2555[8]. Enligt skäl 86 i det direktivet har leverantörer av hanterade 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 hanterade säkerhetstjänster har dock också själva varit mål för cyberattacker och utgör en särskild risk, eftersom de är nära integrerade i sina

[7] 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).

[8] 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).

kunders verksamhet. Väsentliga och viktiga entiteter i den mening som avses i direktiv (EU) 2022/2555 bör därför visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster.

(3) Leverantörer av hanterade säkerhetstjänster spelar också en viktig roll i EU:s cybersäkerhetsreserv, vars gradvisa inrättande stöds av förordning (EU).../.... [om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter]. EU:s cybersäkerhetsreserv ska användas för att stödja insatser samt åtgärder för omedelbar återhämtning i händelse av betydande och storskaliga cybersäkerhetsincidenter. I förordning (EU).../... [om åtgärder för att stärka solidariteten och kapaciteten i unionen för att upptäcka, förbereda sig inför och reagera på cybersäkerhetshot och cyberincidenter] fastställs ett förfarande för urval av leverantörer som ska bilda EU:s cybersäkerhetsreserv, vid vilket det bland annat bör tas hänsyn till huruvida leverantören i fråga har erhållit en europeisk eller nationell cybersäkerhetscertifiering. De relevanta tjänster som tillhandahålls av ”betrodda leverantörer” i enlighet med förordning (EU).../... [om åtgärder för att stärka solidariteten och kapaciteten i unionen för att upptäcka, förbereda sig inför och reagera på cybersäkerhetshot och cyberincidenter] motsvarar ”hanterade säkerhetstjänster” i enlighet med denna förordning.

(4) Certifieringen av hanterade säkerhetstjänster är inte endast relevant för förfarandet för urvalet till EU:s cybersäkerhetsreserv, utan är även en viktig kvalitetsindikator för privata och offentliga entiteter som avser att köpa sådana tjänster. Mot bakgrund av de hanterade säkerhetstjänsternas kritiska karaktär och känsligheten hos de data som de behandlar skulle certifieringen kunna ge potentiella kunder viktig vägledning och visshet i fråga om dessa tjänsters tillförlitlighet. Europeiska certifieringsordningar för hanterade säkerhetstjänster bidrar till att undvika en fragmentering av den inre marknaden. Denna förordning syftar därför till att förbättra den inre marknadens funktion.

(5) Utöver de införda IKT-produkterna, IKT-tjänsterna eller IKT-processerna tillhandahålls genom de hanterade säkerhetstjänsterna ofta ytterligare tjänstefunktioner som är beroende av kompetensen, sakkunskapen och erfarenheten hos deras personal. 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 hanterade säkerhetstjänster som tillhandahålls. För att säkerställa att alla aspekter av en hanterad säkerhetstjänst kan omfattas av en certifieringsordning är det därför nödvändigt att ändra förordning (EU) 2019/881.

Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 och avgav ett yttrande den 11 mars 2021.

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 hanterade 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) Punkterna 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 hanterade 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 och hanterade 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 hanterad säkerhetstjänst har utvärderats för kontroll av överensstämmelse med specifika säkerhetskrav som fastställs i en europeisk ordning för cybersäkerhetscertifiering.

b) Följande led ska införas:

”14a. hanterad säkerhetstjänst: en tjänst som består i att utföra, eller tillhandahålla stöd för, verksamhet som rör hantering av cybersäkerhetsrisker, inbegripet incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster.”

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

”20. *tekniska specifikationer*: 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 hanterad säkerhetstjänst.

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

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

3) I artikel 4 ska punkt 6 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 hanterade 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 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 hanterade säkerhetstjänster, enligt avdelning III i denna förordning, genom att

a) fortlöpande övervaka utvecklingen i fråga om standardisering inom anknutna områden och rekommendera lämpliga tekniska specifikationer för användning vid utveckling av de europeiska ordningarna för cybersäkerhetscertifiering enligt artikel 54.1 c där standarder inte finns tillgängliga,

b) utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (nedan kallade förslag till certifieringsordning) för IKT-produkter och IKT-tjänster, IKT-processer och hanterade säkerhetstjänster, i samarbete med branschen och i enlighet med artikel 49,

c) utvärdera antagna europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 49.8,

d) delta i sakkunnigbedömningar enligt artikel 59.4,

e) bistå kommissionen med att tillhandahålla sekretariatet för europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 62.5.”

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 hanterade 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 hanterade säkerhetstjänster.”

5) I artikel 46 ska punkterna 1 och 2 ersättas med följande:

”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 hanterade säkerhetstjänster.

2. Genom det europeiska ramverket för cybersäkerhetscertifiering ska en mekanism fastställas för inrättandet av europeiska ordningar för cybersäkerhetscertifiering. Den ska 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 hanterade säkerhetstjänster som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgängligheten, autenticiteten, integriteten och konfidentialiteten 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 mycket hög nivå av relevant teknisk kunskap och yrkesintegritet.”

6) I artikel 47 ska punkterna 2 och 3 ersättas med följande:

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

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

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

b) Relevant unionsrätt eller unionspolitik, eller relevant nationell rätt eller nationell politik.

c) Efterfrågan på marknaden.

d) Utvecklingen av hotbilden inom cyberområdet.

e) Begäran om utarbetande av ett specifikt förslag till certifieringsordning av europeiska gruppen för cybersäkerhetscertifiering.”

7) I artikel 49 ska punkt 7 ersättas med följande:

”7. Med utgångspunkt i förslaget till certifieringsordning som Enisa lagt fram, får kommissionen anta genomförandeakter för europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och hanterade säkerhetstjänster som uppfyller kraven i artiklarna 51, 52 och 54. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.”

8) 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 och IKT-processer ska vara utformat för att, i tillämpliga fall, uppnå åtminstone följande säkerhetsmålsättningar:”

9) Följande artikel ska införas:

”Artikel 51a

Säkerhetsmålsättningarna för europeiska ordningar för cybersäkerhetscertifiering för hanterade säkerhetstjänster

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

a) Att säkerställa att de hanterade säkerhetstjänsterna tillhandahålls med den kompetens, sakkunskap och erfarenhet som krävs, inbegripet att den personal som ansvarar för att tillhandahålla dessa tjänster har en mycket hög nivå av teknisk kunskap och kompetens på det specifika området, tillräcklig och lämplig erfarenhet och största möjliga yrkesintegritet.

b) Att säkerställa att leverantören har lämpliga interna förfaranden för att säkerställa att de hanterade säkerhetstjänsterna alltid tillhandahålls med en mycket hög nivå av kvalitet.

c) Att skydda data som är föremål för åtkomst, behandling, lagring eller överföring i samband med tillhandahållandet av hanterade 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 rätt tid vid en fysisk eller teknisk incident.

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

f) Att registrera och möjliggöra 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 säkerställa att de IKT-produkter, IKT-tjänster och IKT-processer [och hårdvara] som används vid tillhandahållandet av de hanterade säkerhetstjänsterna är säkra i sitt grundutförande och är säkra genom sin konstruktion, inte innehåller några kända sårbarheter och inbegriper de senaste säkerhetsuppdateringarna.”

10) 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 hanterade 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 hanterad 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 hanterade 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 och hanterade 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 och hanterade 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 hanterade 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 och hanterade 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 hanterade 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.”

11) I artikel 53 ska punkterna 1, 2 och 3 ersättas med följande:

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

2. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller hanterade 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 hanterade säkerhetstjänster ansvar för att IKT-produkten, IKT-tjänsten, IKT-processen eller den hanterade säkerhetstjänsten överensstämmer med de krav som anges i den ordningen.

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

12) I artikel 54 ska punkt 1 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 och hanterade säkerhetstjänster som omfattas av certifieringsordningen.”

b) Led j ska ersättas med följande:

”j) Reglerna för övervakning av efterlevnaden av IKT-produkter, IKT-tjänster, IKT-processer och hanterade säkerhetstjänster vad gäller kraven i europeiska cybersäkerhetscertifikat eller EU-försäkran om

överensstämmelse, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven.”

c) Led l ska ersättas med följande:

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

d) 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 och hanterade säkerhetstjänster, säkerhetskrav, utvärderingskriterier och utvärderingsmetoder samt assuransnivåer."

e) Led q ska ersättas med följande:

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

13) Artikel 56 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. IKT-produkter, IKT-tjänster, IKT-processer och hanterade 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 hanterade 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 hanterade säkerhetstjänster som ska omfattas av en existerande certifieringsordning som bör täckas av en obligatorisk certifieringsordning.”

ii) Tredje stycket ska ändras på följande sätt:

aa) Led a ska ersättas med följande:

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

bb) 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 hanterade säkerhetstjänster, däribland små och medelstora företag,

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 hanterade säkerhetstjänster för certifiering ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndighet för cybersäkerhetscertifiering som avses i 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 hanterade säkerhetstjänster 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.”

14) I artikel 57 ska punkterna 1 och 2 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 hanterade 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 i enlighet med artikel 49.7. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster, IKT-processer och hanterade 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 hanterade säkerhetstjänster som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.”

15) 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 bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering enligt artikel 54.1 j för övervakning av IKT-produkters, IKT-tjänsters, IKT-processers och hanterade 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 hanterade 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 enligt 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, bland annat genom att utbyta information om IKT-produkter, IKT-tjänster, IKT-processer och hanterade 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 hanterade säkerhetstjänster.”

16) I artikel 59.3 ska leden b och c ersättas med följande:

”b) av förfarandena för övervakning och kontroll av efterlevnaden av bestämmelserna om IKT-produkters, IKT-tjänsters, IKT-processers och hanterade 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 hanterade säkerhetstjänster har i enlighet med artikel 58.7 b,”

17) I artikel 67 ska punkterna 2 och 3 ersättas med följande:

”2. Utvärderingen ska även bedöma effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i denna förordning i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer och hanterade 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 hanterade säkerhetstjänster som inte uppfyller de grundläggande cybersäkerhetskraven kommer in på unionsmarknaden.”

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 Strasbourg den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*