2025/2540

12.12.2025

# KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2540

## af 9. december 2025

## om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår fastlæggelsen af planen for peerreviews

**(EØS-relevant tekst)**

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) ([1]), særlig artikel 59, stk. 5, og

ud fra følgende betragtninger:

(1) I henhold til artikel 59, stk. 4, i forordning (EU) 2019/881 skal peerreviews af nationale cybersikkerhedscertificeringsmyndigheder foretages af to nationale cybersikkerhedscertificeringsmyndigheder fra andre medlemsstater og af Kommissionen. Med henblik på at opnå ensartede standarder for europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer bør Kommissionen overvåge aspekter vedrørende overholdelse af denne forordning og sikre, at peerreviews foretages på en ensartet måde i hele Unionen. For at bidrage til at kortlægge god praksis, udfordringer og erfaringer fra gennemførelsen af europæiske cybersikkerhedscertificeringsordninger bør Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) have mulighed for at deltage i peerreviewene som observatør. For at støtte den harmoniserede gennemførelse af bestemmelserne i denne forordning bør ENISA i samarbejde med Kommissionen og Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG) også have mulighed for at udarbejde modeller.

(2) For at sikre en forudsigelig planlægning og en effektiv ressourcefordeling bør peerreviewene af hver national cybersikkerhedscertificeringsmyndighed foretages i overensstemmelse med en fastlagt tidsplan. Det bør være muligt for en national cybersikkerhedscertificeringsmyndighed at anmode om at udsætte sit peerreview under helt særlige omstændigheder såsom uventet personalemangel eller tilfælde af force majeure. Med henblik herpå er det nødvendigt at fastsætte de nærmere bestemmelser for vurderingen af denne anmodning, så det sikres, at den overordnede tidsplan fastholdes, og at peerreviewmekanismens mål ikke bringes i fare.

(3) For at sikre, at alle medlemsstater bidrager til gennemførelsen af peerreviewmekanismen, og for at sætte dem i stand til at drage fordel af peerlæring bør de nationale cybersikkerhedscertificeringsmyndigheder i hver medlemsstat foretage to peerreviews over en femårig periode. Der bør derfor oprettes en rotationsordning, der gør det muligt for de nationale cybersikkerhedscertificeringsmyndigheder i alle medlemsstater at tilrettelægge deres deltagelse. Det er også nødvendigt at fastsætte kriterier, som de nationale cybersikkerhedscertificeringsmyndigheder bør tage hensyn til, når de udvælger repræsentanter til at foretage peerreviews, med det formål at sikre tilstrækkelig ekspertise og kompetence. De nationale cybersikkerhedscertificeringsmyndigheder bør også have mulighed for at deltage i peerreviews som observatører med henblik på at overvåge og lære af processen. I sådanne tilfælde bør det ikke kræves, at deres repræsentant har samme ekspertise og kompetence som dem, der forventes af de repræsentanter for de nationale cybersikkerhedscertificeringsmyndigheder, som foretager peerreviewene.

(4) For at sikre, at en national cybersikkerhedscertificeringsmyndighed peerreviewes af mindst én national cybersikkerhedscertificeringsmyndighed, der anvender samme tilgang til udstedelse af certifikater på niveau »højt«, bør ENISA, når det opfordrer nationale cybersikkerhedscertificeringsmyndigheder til at tilkendegive deres interesse i at være peerreviewende myndighed, angive, om den peerreviewede nationale cybersikkerhedscertificeringsmyndighed direkte udsteder certifikater på niveau »højt«, gør brug af den model for forudgående godkendelse, der er omhandlet i artikel 56, stk. 6, litra a), i forordning (EU) 2019/881, giver generel delegation i overensstemmelse med nævnte stykkes litra b) eller har en kombination af disse karakteristika.

([1]) EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) For at sikre fælles evalueringskriterier og -procedurer for gennemførelsen af peerreviews i hele Unionen bør hvert peerreview altid omfatte et selvvurderingsspørgeskema, en gennemgang af dokumentation samt et besøg på stedet, herunder interviews. Efter besøget på stedet bør peerreviewholdet drøfte resultaterne med den peerreviewede nationale cybersikkerhedscertificeringsmyndighed, udarbejde et udkast til rapport og forelægge den for den peerreviewede nationale cybersikkerhedscertificeringsmyndighed med henblik på eventuelle bemærkninger, så der sikres konsensus, hvor det er muligt. Peerreviewholdet bør forelægge den endelige rapport, som kan indeholde retningslinjer eller henstillinger for at give den peerreviewede nationale cybersikkerhedscertificeringsmyndighed mulighed for at foretage forbedringer, for ECCG. ECCG bør efter forslag fra peerreviewholdet også godkende en sammenfattende rapport, der skal gøres offentligt tilgængelig.

(6) For at sikre, at de oplysninger, der indhentes som led i peerreviewprocessen, håndteres på en sikker måde, bør peerreviewholdet sørge for, at der anvendes sikre kommunikationskanaler såsom en sikker platform til opbevaring og deling af dokumenter samt anvendes passende sikkerhedsforanstaltninger for fortrolige data, der deles mellem medlemmer af peerreviewholdet. ENISA bør under hensyntagen til de nationale cybersikkerhedscertificeringsmyndigheders eksisterende bedste praksis også kunne udarbejde retningslinjer for, hvordan sikker kommunikation kan garanteres, navnlig med henblik på at sikre, at det sikkerhedsniveau, som peerreviewholdet anvender ved indsamling, udveksling og behandling af oplysninger, er i overensstemmelse med den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds sikkerhedsbehov.

(7) For at lette samarbejdet og en effektiv udveksling af oplysninger mellem de nationale cybersikkerhedscertificeringsmyndigheder bør ECCG, navnlig dens undergruppe vedrørende peerreview, bidrage til udarbejdelsen af modeller samt bistå Kommissionen med gennemførelsen af nærværende forordning.

(8) Peerreviewmekanismen udgør en transeuropæisk digital offentlig tjeneste som omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2024/903 ([2]). Nærværende forordning indfører nye bindende krav, der påvirker nævnte tjeneste, og er som sådan omfattet af forpligtelsen til interoperabilitetsvurdering i henhold til artikel 3 i forordning (EU) 2024/903. Der er derfor foretaget en interoperabilitetsvurdering, og den deraf følgende rapport skal offentliggøres på portalen for et interoperabelt Europa.

(9) Ved udarbejdelsen af nærværende forordning har Kommissionen taget hensyn til ECCG's betragtninger, herunder dens undergruppe vedrørende peerreview.

(10) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 66 i forordning (EU) 2019/881 —

VEDTAGET DENNE FORORDNING:

*Artikel 1*

**Tidsplan, hyppighed og omkostninger i forbindelse med peerreviews**

1. Peerreviewene af de nationale cybersikkerhedscertificeringsmyndigheder foretages i overensstemmelse med den i bilag I fastlagte tidsplan. Hver peerreview afsluttes senest den dato, der er angivet i tidsplanen, og foretages derefter en gang hvert femte år.

2. Under helt særlige omstændigheder kan en peerreviewet national cybersikkerhedscertificeringsmyndighed indgive en behørigt begrundet anmodning til Kommissionen om at udsætte peerreviewet til efter den dato, der er angivet i tidsplanen i bilag I. Kommissionen foretager i samarbejde med Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG), der er oprettet ved artikel 62 i forordning (EU) 2019/881, en vurdering af anmodningen og underretter rettidigt alle relevante parter om resultatet.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2024/903 af 13. marts 2024 om foranstaltninger til sikring af et højt niveau af interoperabilitet i den offentlige sektor i hele Unionen (forordningen om et interoperabelt Europa) (EUT L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Hvis en medlemsstat i overensstemmelse med artikel 58, stk. 1, i forordning (EU) 2019/881 har udpeget:

a) mere end én national cybersikkerhedscertificeringsmyndighed på sit område, foretages der et parallelt peerreview af alle de nationale cybersikkerhedscertificeringsmyndigheder i den pågældende medlemsstat

b) den eller de nationale cybersikkerhedscertificeringsmyndigheder fra en anden medlemsstat, kan denne eller disse nationale cybersikkerhedscertificeringsmyndigheder peerreviewes i overensstemmelse med den tidsplan, der er fastlagt for enten den udpegende medlemsstat eller for den eller de udpegede nationale cybersikkerhedscertificeringsmyndigheders medlemsstat, for så vidt angår de tilsynsopgaver, der udføres i den udpegende medlemsstat.

4. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) offentliggør følgende oplysninger på webstedet om europæiske cybersikkerhedscertificeringsordninger, der er oprettet i henhold til artikel 50 i forordning (EU) 2019/881:

a) oplysningerne om tidsplanen i bilag I

b) den liste over peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, der føres i henhold til artikel 2, stk. 5.

5. Hver national cybersikkerhedscertificeringsmyndighed, der er involveret i peerreviewprocessen, afholder sine egne deltagelsesomkostninger.

*Artikel 2*

**Rotationsordning for peerreviewende nationale cybersikkerhedscertificeringsmyndigheder**

1. I henhold til artikel 59, stk. 4, i forordning (EU) 2019/881 skal hver peerreview foretages af to peerreviewende nationale cybersikkerhedscertificeringsmyndigheder fra andre medlemsstater og af Kommissionen. De nationale cybersikkerhedscertificeringsmyndigheder fra hver medlemsstat deltager i peerreviewet af mindst to nationale cybersikkerhedscertificeringsmyndigheder i hver af de perioder, der er fastsat i bilag I.

2. De nationale cybersikkerhedscertificeringsmyndigheder fra andre medlemsstater kan efter aftale med den peerreviewede nationale cybersikkerhedscertificeringsmyndighed, de peerreviewende nationale cybersikkerhedscertificeringsmyndigheder og Kommissionen deltage i peerreviewet som observatører med en eller flere repræsentanter.

3. En repræsentant for ENISA kan deltage i peerreviewet som observatør. Yderligere repræsentanter kan efter aftale med den peerreviewede nationale cybersikkerhedscertificeringsmyndighed, de peerreviewende nationale cybersikkerhedscertificeringsmyndigheder og Kommissionen også deltage.

4. Observatører skal have adgang til samme oplysninger som de øvrige medlemmer af peerreviewholdet, men må ikke udføre opgaver, der vedrører gennemførelsen af peerreviewet.

5. ENISA foreslår og fører i samarbejde med Kommissionen og ECCG listen over peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, der skal gennemføre den i bilag I fastlagte tidsplan. I løbet af et givet år anmoder ENISA i samarbejde med Kommissionen de nationale cybersikkerhedscertificeringsmyndigheder om at tilkendegive deres interesse i at foretage eller deltage som observatører i de peerreviews af nationale cybersikkerhedscertificeringsmyndigheder, der er fastlagt i tidsplanen i bilag I for det efterfølgende år.

6. Hvis mere end to nationale cybersikkerhedscertificeringsmyndigheder tilkendegiver deres interesse i at foretage peerreviewet af den samme nationale cybersikkerhedscertificeringsmyndighed, hører Kommissionen og ENISA de interesserede nationale cybersikkerhedscertificeringsmyndigheder og træffer afgørelse om, hvem der skal deltage i peerreviewet.

7. Hvis der i et givet år ikke er nok peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, der tilkendegiver deres interesse i at foretage peerreviewene, udvælger Kommissionen efter høring af ECCG de nationale cybersikkerhedscertificeringsmyndigheder, der skal foretage peerreviewene. Ved udvælgelsen tager Kommissionen hensyn til hver medlemsstats nationale cybersikkerhedscertificeringsmyndigheders forpligtelse til at deltage i peerreviewet af mindst to nationale cybersikkerhedscertificeringsmyndigheder, jf. stk. 1.

*Artikel 3*

**Kriterier for sammensætning af peerreviewholdet**

1. I god tid inden indledningen af peerreviewet udpeger hver peerreviewende national cybersikkerhedscertificeringsmyndighed en repræsentant til at foretage peerreviewet. Peerreviewende nationale cybersikkerhedscertificeringsmyndigheder kan udpege mere end én repræsentant, hvis det er nødvendigt for at sikre, at peerreviewholdet har de fornødne kompetencer til at foretage peerreviewet.

2. Repræsentanten for peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, med undtagelse af repræsentanter for nationale cybersikkerhedscertificeringsmyndigheder, der deltager som observatører, skal opfylde følgende kriterier:

a) have mindst to års arbejdserfaring ved den peerreviewende nationale cybersikkerhedscertificeringsmyndighed eller have deltaget i mindst to peerreviews som observatør

b) have tilstrækkeligt kendskab til den ramme for cybersikkerhedscertificering, der er fastsat i forordning (EU) 2019/881

c) have et godt praktisk kendskab til engelsk og, hvor det er muligt, til et eller flere af de sprog, der tales i den medlemsstat, hvor de peerreviewede nationale cybersikkerhedscertificeringsmyndigheder er beliggende

d) fungere uafhængigt af den peerreviewede nationale cybersikkerhedscertificeringsmyndighed.

3. De peerreviewende nationale cybersikkerhedscertificeringsmyndigheder sørger for, at de andre nationale cybersikkerhedscertificeringsmyndigheder, Kommissionen og ENISA underrettes om enhver risiko for interessekonflikt vedrørende de udpegede repræsentanter, inden peerreviewprocessen indledes. Den peerreviewede nationale cybersikkerhedscertificeringsmyndighed kan gøre indsigelse mod udpegelsen af bestemte repræsentanter i overensstemmelse med stk. 5.

4. De peerreviewende nationale cybersikkerhedscertificeringsmyndigheder udvælger indbyrdes en repræsentant (»teamlederen«) til at koordinere peerreviewet.

5. Kommissionen giver den peerreviewede nationale cybersikkerhedscertificeringsmyndighed navnene og kontaktoplysningerne på repræsentanterne for de peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, inden peerreviewprocessen indledes. Hvis den peerreviewede nationale cybersikkerhedscertificeringsmyndighed ønsker at gøre indsigelse mod udpegelsen af en eller flere repræsentanter, giver den inden for to uger Kommissionen en klar begrundelse, underretter ENISA og ECCG og anmoder den peerreviewende nationale cybersikkerhedscertificeringsmyndighed om at udpege en anden repræsentant.

6. Hvis proceduren i stk. 5 medfører unødige forsinkelser i indledningen af peerreviewet på grund af helt særlige omstændigheder, træffer Kommissionen i samråd med ENISA og ECCG afgørelse om sammensætningen af peerreviewholdet.

*Artikel 4*

**Peerreviewmetode**

1. Peerreviewet skal omfatte en vurdering af de aspekter, der er opført i bilag II, i overensstemmelse med artikel 59, stk. 3, i forordning (EU) 2019/881.

2. ENISA kan i samarbejde med ECCG og Kommissionen udarbejde modeller til vurdering af de processer, som den peerreviewede nationale cybersikkerhedscertificeringsmyndighed har fastlagt.

3. Peerreviewet skal omfatte følgende:

a) et selvvurderingsspørgeskema

b) en vurdering af relevant dokumentation

c) online eller fysiske interviews eller begge dele

d) et besøg på stedet.

4. Peerreviewets varighed kan aftales på forhånd mellem peerreviewholdet og den peerreviewede nationale cybersikkerhedscertificeringsmyndighed afhængigt af, hvor store og komplekse den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds aktiviteter er. Besøget på stedet må ikke vare længere end tre arbejdsdage.

5. Medmindre andet aftales mellem peerreviewholdet, den peerreviewede nationale cybersikkerhedscertificeringsmyndighed og Kommissionen, er samarbejdssproget engelsk. Den i artikel 5 omhandlede peerreviewrapport udarbejdes som minimum på engelsk.

6. Den peerreviewede nationale cybersikkerhedscertificeringsmyndighed samarbejder og giver peerreviewholdet adgang til de oplysninger og dokumenter, der er nødvendige for at foretage peerreviewet. Den peerreviewede nationale cybersikkerhedscertificeringsmyndighed indsender selvvurderingsspørgeskemaet og den seneste årlige sammenfattende rapport, der er vedtaget i overensstemmelse med artikel 58, stk. 7, litra g), i forordning (EU) 2019/881, mindst 21 dage før datoen for besøget på stedet. Yderligere dokumenter forelægges efter anmodning fra peerreviewholdet senest syv dage efter modtagelsen af sådanne anmodninger.

7. Dokumenter forelægges på engelsk, medmindre andet er aftalt i henhold til stk. 5. Hvis dokumenterne ikke foreligger på engelsk, kan peerreviewholdet anmode om, at de dokumenter, der er nødvendige for at foretage peerreviewet, oversættes til engelsk.

8. Inden udarbejdelsen af peerreviewrapporten i overensstemmelse med artikel 5 drøfter peerreviewholdet de foreløbige resultater med den peerreviewede nationale cybersikkerhedscertificeringsmyndighed.

*Artikel 5*

**Peerreviewrapport**

1. Senest 21 dage efter gennemførelsen af peerreviewet udarbejder peerreviewholdet et udkast til peerreviewrapport, som skal indeholde nærmere oplysninger om medlemsstaten for den peerreviewede nationale cybersikkerhedscertificeringsmyndighed, de peerreviewende nationale cybersikkerhedscertificeringsmyndigheder, Kommissionen og eventuelle observatører samt resultaterne og konklusionerne af peerreviewet. Hvis det er relevant, skal rapporterne indeholde henstillinger, der gør det muligt at forbedre de aspekter, der er omfattet af peerreviewet.

2. ENISA kan i samarbejde med Kommissionen og ECCG udarbejde en model for peerreviewrapporten.

3. Efter udarbejdelsen af udkastet til peerreviewrapport i overensstemmelse med stk. 1 forelægger peerreviewholdet udkastet for den peerreviewede nationale cybersikkerhedscertificeringsmyndighed med henblik på fremsættelse af eventuelle bemærkninger inden for 14 dage. Peerreviewholdet evaluerer bemærkningerne og integrerer dem om muligt i den endelige rapport, så der sikres konsensus. I tilfælde af uenighed vedlægges den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds svar som bilag til den endelige rapport.

4. Den endelige rapport sendes senest to måneder efter gennemførelsen af peerreviewet til ECCG, herunder et resumé til offentliggørelse. I overensstemmelse med artikel 59, stk. 6, i forordning (EU) 2019/881 gennemgår ECCG rapporten og godkender resuméet heraf, som offentliggøres på webstedet om europæiske cybersikkerhedscertificeringsordninger, der er oprettet i henhold til artikel 50 i forordning (EU) 2019/881. Resuméet skal efter aftale med den peerreviewede nationale cybersikkerhedscertificeringsmyndighed også omfatte den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds svar eller dele heraf.

5. Peerreviewholdet anonymiserer personoplysninger, som det måtte have indsamlet som led i peerreviewet, inden peerreviewrapporten rundsendes uden for peerreviewholdet.

*Artikel 6*

**Fortrolighed**

1. Alle parter, der involveret i peerreviewet, skal overholde tavshedspligten for oplysninger og data, der indhentes som led i udførelsen af deres opgaver og aktiviteter, på en sådan måde, at de navnlig beskytter:

a) intellektuelle ejendomsrettigheder og fysiske eller juridiske personers fortrolige forretningsoplysninger eller forretningshemmeligheder, herunder kildekode, med undtagelse af de tilfælde, der er omhandlet i artikel 5 i Europa-Parlamentets og Rådets direktiv (EU) 2016/943 ([3])

b) den effektive gennemførelse af denne forordning

c) offentlige og nationale sikkerhedsinteresser

d) strafferetlige eller administrative procedurers integritet.

2. Peerreviewholdet sørger for, at alle oplysninger, der indhentes som led i peerreviewprocessen, håndteres sikkert. Når den endelige rapport og resuméet, jf. artikel 5, stk. 4, er udarbejdet, sletter eller destruerer peerreviewholdet, herunder eventuelle observatører, alle dokumenter, bortset fra den endelige rapport og resuméet, der er indsamlet eller genereret som led i peerreviewprocessen.

3. ENISA kan under hensyntagen til de nationale cybersikkerhedscertificeringsmyndigheders eksisterende bedste praksis i samarbejde med ECCG udarbejde retningslinjer for sikker og fortrolig kommunikation.

([3]) Europa-Parlamentets og Rådets direktiv (EU) 2016/943 af 8. juni 2016 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse (EUT L 157 af 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

*Artikel 7*

**Kapacitetsopbygning**

ENISA foretager en analyse af de samlede resultater af peerreviewene og fremhæver de indhentede erfaringer og bedste praksis med henblik på at bidrage til kapacitetsopbygning i de nationale cybersikkerhedscertificeringsmyndigheder og til opretholdelsen af europæiske cybersikkerhedscertificeringsordninger. Denne analyse kan, hvor det er relevant, omfatte uddannelse og yderligere retningslinjer for nationale cybersikkerhedscertificeringsmyndigheder, der er udarbejdet i samarbejde med ECCG.

*Artikel 8*

**Ikrafttræden**

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 9. december 2025.

*På Kommissionens vegne*
Ursula VON DER LEYEN
*Formand*

*BILAG I*

**Tidsplan for nationale cybersikkerhedscertificeringsmyndigheder, der er underlagt peerreview**

Nationale cybersikkerhedscertificeringsmyndigheder i følgende medlemsstater peerreviewes senest den 31. december 2026 og derefter hvert femte år:

Sverige, Belgien, Slovakiet, Tyskland, Malta og Tjekkiet

Nationale cybersikkerhedscertificeringsmyndigheder i følgende medlemsstater peerreviewes senest den 31. december 2027 og derefter hvert femte år:

Ungarn, Grækenland, Estland, Slovenien, Nederlandene og Italien

Nationale cybersikkerhedscertificeringsmyndigheder i følgende medlemsstater peerreviewes senest den 31. december 2028 og derefter hvert femte år:

Kroatien, Danmark, Litauen, Spanien, Bulgarien og Irland

Nationale cybersikkerhedscertificeringsmyndigheder i følgende medlemsstater peerreviewes senest den 31. december 2029 og derefter hvert femte år:

Finland, Østrig, Rumænien, Luxembourg, Letland og Polen

Nationale cybersikkerhedscertificeringsmyndigheder i følgende medlemsstater og EØS/EFTA-lande peerreviewes senest den 31. december 2030 og derefter hvert femte år:

Cypern, Frankrig, Portugal, Liechtenstein, Norge og Island

*BILAG II*

## Peerreviewmetode

### II.1 Opdeling mellem certificerings- og tilsynsaktiviteter

Ved vurderingen af opdelingen mellem certificeringsaktiviteterne og tilsynsaktiviteterne i den peerreviewede nationale cybersikkerhedscertificeringsmyndighed, jf. artikel 59, stk. 3, litra a), i forordning (EU) 2019/881, skal peerreviewet som minimum omfatte en vurdering af følgende aspekter:

a) en detaljeret beskrivelse af, hvordan den peerreviewede nationale cybersikkerhedscertificeringsmyndighed fungerer, med tydelig angivelse af de forskellige enheder og/eller afdelinger, der er involveret i gennemførelsen af forordning (EU) 2019/881

b) en kortlægning af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds aktiviteter i forhold til de aktiviteter, der er opført i artikel 58, stk. 7, i forordning (EU) 2019/881

c) hvis den peerreviewede nationale cybersikkerhedscertificeringsmyndighed udsteder certifikater, en redegørelse for, at der ikke er nogen interferens mellem dens certificeringsaktiviteter og tilsynsaktiviteterne, jf. litra b).

### II.2 Tilsyn med og håndhævelse af reglerne for kontrol med overholdelsen af certifikaterne

Ved vurderingen af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds procedurer for tilsyn med og håndhævelse af reglerne for overvågning af, at IKT-produkter, IKT-tjenester, IKT-processer og administrerede sikkerhedstjenester overholder europæiske cybersikkerhedsattester, jf. artikel 59, stk. 3, litra b), i forordning (EU) 2019/881, skal peerreviewet som minimum omfatte en vurdering af følgende aspekter:

a) kvaliteten og detaljeringsgraden af beskrivelsen af sådanne processer og procedurer, og i hvilket omfang de er dokumenteret

b) hvorvidt og i hvilket omfang sådanne processer og procedurer omfatter de relevante europæiske cybersikkerhedscertificeringsordninger

c) hvorvidt den peerreviewede nationale cybersikkerhedscertificeringsmyndighed reelt har beføjelse til at inspicere overensstemmelsesvurderingsorganer, der udsteder certifikater, og om nødvendigt til at håndhæve inddragelsen af certifikater

d) omfanget af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds samarbejde med de relevante markedsovervågningsmyndigheder

e) hvorvidt den peerreviewede nationale cybersikkerhedscertificeringsmyndighed har en mekanisme til at behandle klager fra fysiske eller juridiske personer, jf. artikel 58, stk. 7, litra f), i forordning (EU) 2019/881, herunder dokumentation for, hvorvidt fysiske og juridiske personer har ret til at indgive en klage og få adgang til effektive retsmidler i overensstemmelse med henholdsvis artikel 63 og 64 i nævnte forordning.

### II.3 Overvågning og håndhævelse af producenters eller udbyderes forpligtelser

Ved vurderingen af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds procedurer for overvågning og håndhævelse af de forpligtelser, der påhviler producenter eller udbydere, som foretager selvvurdering af overensstemmelse, jf. artikel 59, stk. 3, litra c), i forordning (EU) 2019/881, skal peerreviewet som minimum omfatte en vurdering af følgende aspekter:

a) hvorvidt den peerreviewede nationale cybersikkerhedscertificeringsmyndighed har fastlagt sådanne procedurer, og i hvilket omfang de er dokumenteret, navnlig om den har etableret en mekanisme til at modtage og behandle oplysninger fra eksterne kilder

b) hvorvidt og i hvilket omfang sådanne procedurer omfatter de relevante europæiske cybersikkerhedscertificeringsordninger

c) hvorvidt og i hvilket omfang den peerreviewede nationale cybersikkerhedscertificeringsmyndighed udfører sine egne undersøgelser, og hvorvidt omfanget af undersøgelserne omfatter producenternes forpligtelser som fastsat i artikel 53, stk. 2 og 3, i forordning (EU) 2019/881 og i de tilsvarende europæiske cybersikkerhedscertificeringsordninger

d) hvorvidt der er en procedure for udveksling af oplysninger inden for rammerne af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds certificeringsaktiviteter og tilsynsaktiviteter, som er relevante for overvågning og håndhævelse af producenters eller udbyderes forpligtelser.

II.4 **Overvågning og godkendelse af og tilsyn med overensstemmelsesvurderingsorganer**

Ved vurderingen af den peerreviewede nationale cybersikkerhedscertificeringsmyndigheds procedurer for overvågning og godkendelse af og tilsyn med overensstemmelsesvurderingsorganers aktiviteter, jf. artikel 59, stk. 3, litra d), i forordning (EU) 2019/881, skal peerreviewet som minimum omfatte en vurdering af følgende aspekter:

a) kvaliteten og detaljeringsgraden af beskrivelsen af sådanne procedurer, og i hvilket omfang de er dokumenteret, herunder med henblik på samarbejde med det nationale akkrediteringsorgan

b) de vigtigste statistikker over antallet af udstedte, suspenderede eller inddragne bemyndigelser, det samlede antal aktive overensstemmelsesvurderingsorganer, antallet af udstedte certifikater og antallet af korrigerende foranstaltninger, som den peerreviewede nationale cybersikkerhedscertificeringsmyndighed har truffet

c) hvis den peerreviewede nationale cybersikkerhedscertificeringsmyndighed tillader udstedelse af europæiske cybersikkerhedsattester på niveau »højt« efter forudgående godkendelse eller på grundlag af en generel delegation af opgaven, jf. artikel 56, stk. 6, i forordning (EU) 2019/881, personalets ekspertise og de procedurer, hvorigennem den peerreviewede nationale cybersikkerhedscertificeringsmyndighed overvåger og fører tilsyn med overensstemmelsesvurderingsorganernes aktiviteter.