2025/295

13.2.2025

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2025/295

af 24. oktober 2024

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder for harmonisering af de betingelser, der muliggør udførelsen af tilsynsaktiviteter

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 ([1]), særlig artikel 41, stk. 2, andet afsnit, og

ud fra følgende betragtninger:

(1) Med rammen for digital operationel modstandsdygtighed i den finansielle sektor, der er oprettet ved forordning (EU) 2022/2554, indføres der en EU-tilsynsramme for tredjepartsudbydere, som leverer informations- og teknologitjenester (IKT-tjenester) til den finansielle sektor og er udpeget som kritiske i overensstemmelse med nævnte forordnings artikel 31.

(2) En tredjepartsudbyder af IKT-tjenester, som beslutter at indgive en frivillig anmodning om at blive udpeget som kritisk, bør for den modtagende europæiske tilsynsmyndighed (ESA) forelægge alle nødvendige oplysninger for at dokumentere sin kritiske betydning i henhold til de principper og kriterier, der er fastsat i forordning (EU) 2022/2554. Af samme årsag bør de oplysninger, der skal indgå i ansøgningen om frivillig anmodning, være tilstrækkeligt udførlige og fuldstændige til at muliggøre en klar og fuldstændig vurdering af kritisk betydning i henhold til nævnte forordnings artikel 31, stk. 11. Den pågældende ESA bør afvise ufuldstændige ansøgninger og anmode om de manglende oplysninger.

(3) Den juridiske identifikation af tredjepartsudbydere af IKT-tjenester inden for rammerne af denne reguleringsmæssige tekniske standard bør tilpasses til den identifikationskode, der er fastsat i Kommissionens gennemførelsesforordning, som er vedtaget i overensstemmelse med artikel 28, stk. 9, i forordning (EU) 2022/2554.

(4) Som opfølgning på de henstillinger, som den ledende tilsynsførende udsteder til kritiske tredjepartsudbydere af IKT-tjenester, bør den ledende tilsynsførende føre tilsyn med, at kritiske tredjepartsudbydere af IKT-tjenester overholder henstillingerne. Med henblik på at sikre effektiv og virkningsfuld overvågning af de tiltag eller de afhjælpende foranstaltninger, som de kritiske tredjepartsudbydere af IKT-tjenester har iværksat/truffet i relation til disse henstillinger, bør den ledende tilsynsførende have mulighed for at kræve de rapporter, der er omhandlet i artikel 35, stk. 1, litra c), i forordning (EU) 2022/2554, og som skal betragtes som midlertidige statusrapporter og endelige rapporter.

(5) Med henblik på den vurdering, der er nærmere beskrevet i artikel 42, stk. 1, i forordning (EU) 2022/2554, i henhold til hvilken den ledende tilsynsførende er forpligtet til at evaluere, hvorvidt redegørelsen fra den kritiske tredjepartsudbyder af IKT-tjenester er tilstrækkelig, bør meddelelsen fra den kritiske tredjepartsudbyder af IKT-tjenester til den ledende tilsynsførende om, at førstnævnte agter at følge de modtagne henstillinger, suppleres af en beskrivelse af de tiltag og foranstaltninger, der er iværksat/truffet for at mindske de risici, der er beskrevet i henstillingerne, sammen med de respektive frister herfor. En sådan redegørelse bør have form af en udbedringsplan.

(6) Idet den ledende tilsynsførende forventes at vurdere de underentrepriseordninger, som den kritiske tredjepartsudbyder af IKT-tjenester er omfattet af, skal der udarbejdes en model til forelæggelse af oplysninger om sådanne ordninger. I modellen skal der tages højde for det forhold, at de kritiske tredjepartsudbydere af IKT-tjenester har strukturer, som er forskellige fra finansielle enheders strukturer.

([1]) EUT L 333 af 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Så snart den ledende tilsynsførende har udstedt henstillinger til en kritisk tredjepartsudbyder af IKT-tjenester og de kompetente myndigheder har underrettet de relevante finansielle enheder om de risici, der er identificeret i nævnte henstillinger, bør den ledende tilsynsførende føre tilsyn med og vurdere den gennemførelse, som den kritiske tredjepartsudbyder af IKT-tjenester foretager af de tiltag og foranstaltninger, der er iværksat/truffet for at efterleve henstillingerne. De kompetente myndigheder bør føre tilsyn med og vurdere, i hvilket omfang de finansielle enheder er eksponeret for de risici, der er identificeret i disse henstillinger. Med det formål at opretholde lige vilkår, samtidig med at de varetager deres respektive opgaver — navnlig når de risici, der er identificeret i henstillingerne, er alvorlige og fælles for en lang række finansielle enheder i flere medlemsstater — bør både de kompetente myndigheder og den ledende tilsynsførende udveksle relevante konklusioner, som er nødvendige for, at de kan varetage deres respektive opgaver. Formålet med udvekslingen af oplysninger er at sikre, at den ledende tilsynsførendes feedback til den kritiske tredjepartsudbyder af IKT-tjenester vedrørende de tiltag og foranstaltninger, som sidstnævnte gennemfører, tager hensyn til deres indvirkning på de finansielle enheders risici, og at de kompetente myndigheders tilsynsaktiviteter tager udgangspunkt i den vurdering, som den ledende tilsynsførende har foretaget.

(8) For at muliggøre en effektiv og virkningsfuld udveksling af oplysninger bør de kompetente myndigheder som led i deres tilsynsaktiviteter vurdere, i hvilket omfang de finansielle enheder, som de fører tilsyn med, er eksponeret for de risici, der er identificeret i henstillingerne. Denne vurdering bør foretages efter en risikobaseret tilgang, der står i rimeligt forhold til formålet. Den ledende tilsynsførende bør anmode de kompetente myndigheder om at udveksle resultaterne af denne vurdering i de specifikke tilfælde, hvor de risici, der er forbundet med henstillingerne, er alvorlige og fælles for en lang række finansielle enheder i flere medlemsstater. Når den ledende tilsynsførende anmoder om forelæggelse af resultaterne af denne vurdering, bør denne — for at gøre bedst mulig brug af de kompetente myndigheders ressourcer — altid tage hensyn til det forhold, at formålet med disse anmodninger er at evaluere gennemførelsen af tiltag og afhjælpende foranstaltninger, som de kritiske tredjepartsudbydere af IKT-tjenester har iværksat/truffet.

(9) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([2]) og afgav en positiv udtalelse den 22. juli 2024.

(10) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som ESA'erne har forelagt for Kommissionen.

(11) Det Fælles Udvalg af ESA'er har afholdt åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, de har analyseret de potentielle omkostninger og fordele herved og anmodet om rådgivning fra interessentgruppen for banker, der er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([3]), interessentgruppen for forsikrings- og genforsikringsordninger og interessentgruppen for arbejdsmarkedspensionsordninger, der er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([4]), og interessentgruppen for værdipapirer og markeder, der er nedsat i henhold til artikel 37 i Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([5]) —

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

([3]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

VEDTAGET DENNE FORORDNING:

Artikel 1

Oplysninger, som tredjepartsudbyderen af IKT-tjenester skal forelægge i sin ansøgning om frivillig anmodning om at blive udpeget som kritisk

1. Tredjepartsudbyderen af informations- og teknologitjenester (IKT-tjenester) skal forelægge følgende oplysninger i sin begrundede ansøgning om frivillig anmodning, jf. artikel 31, stk. 11, i forordning (EU) 2022/2554, om at blive udpeget som kritisk i henhold til artikel 31, stk. 1, litra a), i forordning (EU) 2022/2554:

a) den juridiske enheds navn

b) den juridiske enheds identifikationskode

c) kontaktpersonens navn og kontaktpunkt for den kritiske tredjepartsudbyder af IKT-tjenester

d) landet, hvor den juridiske enhed har sit vedtægtsmæssige hjemsted

e) en beskrivelse af koncernstrukturen, herunder som minimum oplysninger om dens modervirksomhed og andre tilknyttede virksomheder, som leverer IKT-tjenester til finansielle enheder i EU. Nævnte oplysninger skal, når det er relevant, inkludere:

   i) de juridiske enheders navne

   ii) den juridiske enheds identifikationskode

   iii) landet, hvor den juridiske enhed har sit vedtægtsmæssige hjemsted

f) et skøn over den markedsandel, som tredjepartsudbyderen af IKT-tjenester besidder i Unionens finansielle sektor, og et skøn over typen af markedsandel efter finansiel enhed, jf. artikel 2, stk. 1, i forordning (EU) 2022/2554, fra året for indgivelse af ansøgningen om at blive udpeget som kritisk og året forud for nævnte ansøgning

g) en beskrivelse af hver af de IKT-tjenester, der leveres til finansielle enheder i Unionen, herunder:

   i) en beskrivelse af virksomhedens art og den type af IKT-tjenester, der leveres til finansielle enheder

   ii) en liste over de funktioner i finansielle enheder, som understøttes af de leverede IKT-tjenester, hvis sådanne findes

   iii) oplysninger om, hvorvidt de IKT-tjenester, der leveres til finansielle enheder, understøtter kritiske eller vigtige funktioner, hvis sådanne findes

h) en liste over finansielle enheder, der gør brug af de IKT-tjenester, som tredjepartsudbyderen af IKT-tjenester leverer, herunder følgende oplysninger for hver af de modtagende finansielle enheder, hvis sådanne foreligger:

   i) den juridiske enheds navn

   ii) den juridiske enheds identifikationskode, hvis tredjepartsudbyderen af IKT-tjenester kender den

   iii) typen af finansiel enhed, jf. artikel 2, stk. 1, i forordning (EU) 2022/2554

   iv) den geografiske beliggenhed, hvorfra IKT-tjenesterne leveres til denne specifikke juridiske enhed

i) en liste over de kritiske tredjepartsudbydere af IKT-tjenester, som indgår i den seneste foreliggende liste over sådanne udbydere offentliggjort af ESA'erne i henhold til artikel 31, stk. 9, i forordning (EU) 2022/2554, og som er afhængige af de tjenester, der leveres af ansøgeren, hvis en sådan foreligger

j) en selvevaluering af følgende:

   i) graden af substituerbarhed for af de IKT-tjenester, som ansøgeren leverer, idet der tages hensyn til følgende:

      — den markedsandel, som tredjepartsudbyderen af IKT-tjenester besidder i Unionens finansielle sektor

— antallet af kendte relevante konkurrenter efter typen af IKT-tjenester eller gruppen af IKT-tjenester

— en beskrivelse af særlige forhold vedrørende de leverede IKT-tjenester, herunder i forbindelse med eventuelle egne teknologier, eller de særlige kendetegn ved tredjepartsudbyderen af IKT-tjenesters organisation eller aktivitet

ii) kendskab til, om der findes alternative tredjepartsudbydere af IKT-tjenester, som kan levere de samme IKT-tjenester som den tredjepartsudbyder af IKT-tjenester, der indgiver ansøgningen

k) oplysninger om en fremtidig forretningsstrategi, som vedrører leveringen af IKT-tjenester og infrastrukturen i finansielle enheder i Unionen, herunder eventuelle planlagte ændringer i koncernen eller ledelsesstrukturen, adgangen til nye markeder eller aktiviteter

l) identifikation af de underleverandører til den tredjepartsudbyder af IKT-tjenester, som er blevet udpeget som kritiske tredjepartsudbydere af IKT-tjenester

m) eventuelle andre begrundelser med relevans for ansøgningen fra tredjepartsudbyderen af IKT-tjenester om at blive udpeget som kritisk.

2. Hvis tredjepartsudbyderen af IKT-tjenester indgår i en koncern, skal oplysningerne i stk. 1 i forelægges i relation til de IKT-tjenester, der leveres af koncernen som helhed.

Artikel 2

Indhold, struktur og format af de oplysninger, som tredjepartsudbydere af IKT-tjenester skal forelægge, offentliggøre eller aflægge rapport om

1. Kritiske tredjepartsudbydere af IKT-tjenester skal efter anmodning fra den ledende tilsynsførende forelægge de oplysninger, som er nødvendige for, at den ledende tilsynsførende kan varetage sine tilsynsopgaver i overensstemmelse med kravene i forordning (EU) 2022/2554.

2. De i stk. 1 omhandlede oplysninger inkluderer blandt andet følgende:

a) oplysninger om ordninger, der er indgået mellem, og kopier af kontraktlige dokumenter for:

i) den kritiske tredjepartsudbyder af IKT-tjenester og finansielle enheder, jf. artikel 2, stk. 1, i forordning (EU) 2022/2554

ii) den kritiske tredjepartsudbyder af IKT-tjenester og dennes underleverandører med henblik på at afspejle den teknologiske værdikæde for de IKT-tjenester, der leveres til finansielle enheder i Unionen

b) oplysninger om organisations- og koncernstrukturen hos den kritiske tredjepartsudbyder af IKT-tjenester, herunder identifikation alle de enheder, der tilhører den samme koncern, som direkte eller indirekte leverer IKT-tjenester til finansielle enheder i Unionen

c) oplysninger om de større aktionærer, herunder deres struktur og geografiske spredning, for alle følgende:

i) enheder, der alene eller sammen med deres tilknyttede enheder, besidder 25 % eller mere af kapitalen eller stemmerettighederne i den kritiske tredjepartsudbyder af IKT-tjenester

ii) enheder, der har rettigheder til udnævnelse eller afsættelse af et flertal af medlemmerne af administrations-, ledelses- eller tilsynsorganet i den kritiske tredjepartsudbyder af IKT-tjenester

iii) enheder, der i henhold til en aftale, udøver kontrol med et flertal af aktionærers eller medlemmers stemmerettigheder i den kritiske tredjepartsudbyder af IKT-tjenester

d) oplysninger om den markedsandel, som den kritiske tredjepartsudbyder af IKT-tjenester besidder, efter typen af tjenester, i de relevante markeder, hvor den driver virksomhed

e) oplysninger om de interne ledelsesordninger i den kritiske tredjepartsudbyder af IKT-tjenester, herunder strukturen med linjer for forvaltningsansvar og regler om ansvarliggørelse

f) referaterne fra ledelsesorganet og eventuelle relevante interne udvalg i kritiske tredjepartsudbydere af IKT-tjenester, som på en hvilken som helst måde vedrører aktiviteter og risici forbundet med IKT-tredjepartstjenester, som understøtter funktioner i finansielle enheder i Unionen

g) oplysninger om IKT-sikkerheden hos den kritiske tredjepartsudbyder af IKT-tjenester, herunder relevante strategier, mål, politikker, procedurer, processer, kontrolforanstaltninger til beskyttelse af følsomme data, adgangskontroller, krypteringspraksis, indsatsplaner i forbindelse med hændelser og oplysninger om overholdelse af relevante regler samt nationale og internationale standarder, hvis det er relevant

h) oplysninger om tekniske og organisatoriske foranstaltninger til sikring af databeskyttelse og fortroligheden af data, herunder personoplysninger og andre data end personoplysninger, gennemførte kontrolforanstaltninger til beskyttelse af følsomme data, adgangskontroller, krypteringspraksis, indsatsplaner i forbindelse med databrud såfremt tredjepartsudbyderen af IKT-tjenester med hensyn til behandling af personoplysninger er omfattet af love fra tredjelande, herunder adgangsanmodninger fra regeringer i tredjelande, en liste over lande og gældende love

i) oplysninger om de mekanismer, som den kritiske tredjepartsudbyder af IKT-tjenester udbyder til finansielle enheder i Unionen for dataportabilitet, applikationsportabilitet og interoperabilitet

j) oplysninger om beliggenheden af datacentre og IKT-produktionscentre, som anvendes med henblik på levering af tjenester til de finansielle enheder, herunder en liste over alle relevante lokaler og faciliteter, som tilhører den kritiske tredjepartsudbyder af IKT-tjenester, også uden for Unionen

k) oplysninger om levering af tjenester, som foretages af den kritiske tredjepartsudbyder af IKT-tjenester fra tredjelande, herunder oplysninger om relevante retlige bestemmelser, som gælder for personoplysninger og andre data end personoplysninger, som behandles af tredjepartsudbyderen af IKT-tjenester

l) oplysninger om foranstaltninger, der træffes for at mindske risici, som hidrører fra leveringen af IKT-tjenester, som foretages af den kritiske tredjepartsudbyder af IKT-tjenester og dennes underleverandører fra tredjelande

m) oplysninger om rammen for risikostyring og rammen for styring af hændelser, herunder politikker, procedurer, værktøjer, mekanismer og forvaltningsordninger hos den kritiske tredjepartsudbyder af IKT-tjenester og dens underleverandører, herunder en liste og beskrivelse af større hændelser med en direkte eller indirekte indvirkning på finansielle enheder i Unionen, som bl.a. omfatter relevante udførlige oplysninger, der tjener til at fastslå hændelsens betydning for finansielle enheder og vurdere mulige grænseoverskridende virkninger

n) oplysninger om rammen for styring af ændringer, herunder politikker, procedurer og kontroller med den kritiske tredjepartsudbyder af IKT-tjenester og dens underleverandører

o) oplysninger om den overordnede indsats- og genopretningsramme hos den kritiske tredjepartsudbyder af IKT-tjenester, som bl.a. omfatter planer for driftsstabiliteten og dermed forbundne ordninger og procedurer, livcykluspolitikker vedrørende softwareudvikling, indsats- og genopretningsplaner og dermed forbundne ordninger og procedurer samt politikker, ordninger og procedurer for sikkerhedskopiering

p) oplysninger om overvågning af ydeevne, sikkerhedsovervågning og sporing af hændelser samt oplysninger om indberetningsmekanismer, som vedrører udførelse af tjenester, hændelser og overholdelse af serviceniveauaftaler og serviceniveaumål eller lignende ordninger mellem kritiske tredjepartsudbydere af IKT-tjenester og finansielle enheder i Unionen

q) oplysninger om rammen for styring af IKT-tredjeparter hos den kritiske tredjepartsudbyder af IKT-tjenester, herunder strategier, politikker, procedurer, processer og kontroller, hvilket bl.a. omfatter udførlige oplysninger om den due diligence og risikovurdering, der foretages af den kritiske tredjepartsudbyder af IKT-tjenester over for dens underleverandører inden de indgår en aftale med dem for at overvåge forholdet, hvilket omfatter alle relevante IKT- og modpartsrisici

r) udskrifter fra overvågnings- og scanningssystemer hos den kritiske tredjepartsudbyder af IKT-tjenester og hos dens underleverandører, hvilket omfatter, men ikke er begrænset til netværks-, server- og applikationsovervågning, sårbarhedsscanning, logstyring, overvågning af ydeevne, styring af hændelser og målinger sat i forhold til pålidelighedsmål, f.eks. serviceniveaumål

s) udskrifter fra produktions-, præproduktions- og testsystemer eller -applikationer, som den kritiske tredjepart-sudbyder af IKT-tjenester og dens underleverandører anvender til direkte eller indirekte at levere tjenester til finansielle enheder i Unionen

t) overensstemmelsesrapporter og tilgængelige revisionsrapporter samt eventuelle relevante revisionsresultater, hvilket bl.a. omfatter revisioner, der udføres af nationale myndigheder i og uden for Unionen, hvor en sådan udveksling af oplysninger er fastsat i samarbejdsaftaler, eller certificeringer, som den kritiske tredjepartsudbyder af IKT-tjenester eller dens underleverandører har opnået, herunder rapporter fra interne og eksterne revisorer, certificeringer eller overensstemmelsesvurderinger med industrispecifikke standarder. Dette inkluderer oplysninger om enhver type tilgængelig uafhængig test af modstandsdygtighed i IKT-systemer hos den kritiske tredjepartsudbyder af IKT-tjenester, herunder enhver type trusselsbaseret penetrationstest, som udføres af tredjepartsudbyderen af IKT-tjenester

u) oplysninger om eventuelle vurderinger, som den kritiske tredjepartsudbyder af IKT-tjenester har foretaget efter dennes anmodning eller på dennes vegne, som evaluerer egnetheden og integriteten af individer, som bestrider vigtige stillinger inden for den kritiske tredjepartsudbyder af IKT-tjenester

v) oplysninger om eventuelle udbedringsplaner, som skal imødekomme henstillinger i henhold til artikel 3 og relevante dertil knyttede oplysninger, som skal bekræfte, at der er gennemført afhjælpende foranstaltninger

w) oplysninger om tilgængelige kursusordninger og programmer til bevidstgørelse om sikkerhed for medarbejdere, herunder, hvis det er relevant, oplysninger om investeringer, ressourcer og metoder, som den kritiske tredjepart-sudbyder af IKT-tjenester anvender til at uddanne sit personale i at håndtere følsomme finansielle data og opretholde høje sikkerhedsniveauer

x) oplysninger om de aktiviteter, som den kritiske tredjepartsudbyder af IKT-tjenester udøver, og finansielle regnskaber, herunder oplysninger om budgettet og ressourcer, som vedrører IKT og sikkerhed.

Artikel 3

Oplysninger fra kritiske tredjepartsudbydere af IKT-tjenester efter udstedelsen af henstillinger

1. Den kritiske tredjepartsudbyder af IKT-tjenester skal for den ledende tilsynsførende forelægge en rapport, som indeholder en udbedringsplan vedrørende de henstillinger og afhjælpende foranstaltninger, som den kritiske tredjepart-sudbyder af IKT-tjenester planlægger at gennemføre for at mindske de risici, der er identificeret i henstillingerne, jf. artikel 35, stk. 1, litra d), i forordning (EU) 2022/2254. Rapporten skal stemme overens med de frister, som den ledende tilsynsførende har fastsat for hver henstilling.

2. For at muliggøre overvågning af gennemførelsen af de tiltag eller de afhjælpende foranstaltninger, som den kritiske tredjepartsudbyder af IKT-tjenester har iværksat/truffet i relation til de modtagne henstillinger, skal den kritiske tredjepart-sudbyder af IKT-tjenester efter anmodning fra den ledende tilsynsførende udveksle følgende med denne:

a) midlertidige statusrapporter og dertil knyttet dokumentation, som præciserer fremskridtene med gennemførelsen af de tiltag og foranstaltninger, der er angivet i den rapport, som den kritiske tredjepartsudbyder af IKT-tjenester har forelagt for den ledende tilsynsførende inden for de af den ledende tilsynsførende fastsatte frister

b) endelige rapporter og dertil knyttet dokumentation, som præciserer de tiltag eller de afhjælpende foranstaltninger, som den kritiske tredjepartsudbyder af IKT-tjenester har iværksat/truffet for at mindske de risici, der er identificeret i de modtagne henstillinger.

Artikel 4

Struktur og format af de oplysninger, som tredjepartsudbydere af IKT-tjenester skal forelægge

1. Den kritiske tredjepartsudbyder af IKT-tjenester skal forelægge de ønskede oplysninger for den ledende tilsynsførende gennem de dertil indrettede sikre elektroniske kanaler som angivet af den ledende tilsynsførende i dennes anmodning og i den form, som den ledende tilsynsførende har angivet.

2. Når den kritiske tredjepartsudbyder af IKT-tjenester forelægger oplysninger for den ledende tilsynsførende, skal denne:

a) følge den struktur, som den ledende tilsynsførende har angivet i sin anmodning om oplysninger

b) klart angive, hvor den relevante oplysning findes i den forelagte dokumentation.

3. De oplysninger, som den kritiske tredjepartsudbyder af IKT-tjenester har forelagt, offentliggjort eller aflagt rapport om til den ledende tilsynsførende, skal være på et sprog, der er almindelig anvendt inden for international finans.

Artikel 5

Model til forelæggelse af oplysninger om underentrepriseordninger

En kritisk tredjepartsudbyder af IKT-tjenester, som er forpligtet til at udveksle oplysninger om underentrepriseordninger, skal forelægge oplysningerne for den ledende tilsynsførende i henhold til den model, der foreligger i bilaget.

Artikel 6

De kompetente myndigheders vurdering af de risici, der er omhandlet i den ledende tilsynsførendes henstillinger

1. Som led i deres tilsyn med finansielle enheder skal de kompetente myndigheder vurdere indvirkningen på de finansielle enheder af de foranstaltninger, som den kritiske tredjepartsudbyder af IKT-tjenester har truffet på grundlag af henstillinger fra den ledende tilsynsførende i overensstemmelse med proportionalitetsprincippet.

2. Når den kompetente myndighed foretager den i stk. 1 omhandlede vurdering, skal den tage hensyn til alle følgende:

a) tilstrækkeligheden og sammenhængen af de korrigerende og afhjælpende foranstaltninger, som de finansielle enheder har gennemført for at mindske de risici, der er identificeret i henstillingerne

b) den vurdering, som den ledende tilsynsførende har foretaget af, hvorvidt den kritiske tredjepartsudbyder af IKT-tjenester overholder de foranstaltninger og tiltag, som indgår i rapporten, hvor dette har virkninger for eksponeringen hos de finansielle enheder, som hører under dens ansvarsområde, for de risici, der er identificeret i henstillingerne

c) holdningen hos andre kompetente myndigheder, som er blevet hørt i overensstemmelse med artikel 42, stk. 5, i forordning (EU) 2022/2554

d) hvorvidt den ledende tilsynsførende anser de tiltag og foranstaltninger, som den kritiske tredjepartsudbyder af IKT-tjenester har gennemført, som tilstrækkelige med henblik til at mindske eksponeringen hos de finansielle enheder, der hører under dens ansvarsområde, for de risici, der er identificeret i henstillingerne.

3. Efter anmodning fra den ledende tilsynsførende skal den kompetente myndighed inden for en rimelig frist forelægge resultaterne af den i stk. 1 omhandlede vurdering. Når den ledende tilsynsførende anmoder om resultaterne af denne vurdering, skal denne tage hensyn til proportionalitetsprincippet og omfanget af de risici, der er forbundet med henstillingerne, herunder de grænseoverskridende virkninger af disse risici, når de har indvirkning på finansielle enheder, der driver virksomheder i mere end én medlemsstat.

4. Når det er relevant, skal den kompetente myndighed anmode finansielle enheder om at forelægge alle nødvendige oplysninger med henblik på at foretage den i stk. 1 omhandlede vurdering.

Artikel 7

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 24. oktober 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

MODEL TIL UDVEKSLING AF OPLYSNINGER OM UNDERENTREPRISEORDNINGER

Oplysningskategori	Elementer af centrale oplysninger
Generelle oplysninger	— Navnet på den kritiske tredjepartsudbyder af IKT-tjenester — Identifikationskode for den kritiske tredjepartsudbyder af IKT-tjenester — Kontaktpersonens navn og kontaktpunkt for den kritiske tredjepartsudbyder af IKT-tjenester — Dato for indgivelse af modellen
Oversigt over underentrepriseordninger	— Et samlet overblik over underentrepriseordningerne, herunder en kort beskrivelse af underentrepriseforholdenes formål og rækkevidde (hvilket bl.a. omfatter en angivelse af underentrepriseordningernes niveau af kritisk betydning og vigtighed for den kritiske tredjepartsudbyder af IKT-tjenester) — En præcisering og beskrivelse af typerne af udliciterede IKT-tjenester og deres væsentlighed for de IKT-tjenester, der leveres til finansielle enheder, i overensstemmelse med de gennemførelsesmæssige tekniske standarder, der er vedtaget i henhold til artikel 28, stk. 9, i forordning (EU) 2022/2554 — Når typerne af IKT-tjenester præciseres, henvises der til listen i bilag IV i de gennemførelsesmæssige tekniske standarder, der er vedtaget i henhold til artikel 28, stk. 9, i forordning (EU) 2022/2554
Oplysninger om underleverandører	— Navn på og nærmere oplysninger om den juridiske enhed (inkl. identifikationskode) for hver underleverandør — Kontaktoplysninger for de medarbejdere, som har ansvar for hver af underentrepriseforholdene i ledelsesstrukturen hos den kritiske tredjepartsudbydere af IKT-tjenester — En oversigt for hver enkelt underleverandør over den ekspertise, erfaring og de kvalifikationer, der vedrører de udliciterede IKT-tjenester
Beskrivelse af tjenester, der leveres af underleverandører	— Udførlig beskrivelse af de specifikke IKT-tjenester, som leveres af hver enkelt underleverandør — Opdeling af de ansvarsområder og de opgaver, som er overdraget til underleverandører, idet de forskellige roller i IKT-processernes forskellige faser beskrives nærmere — Oplysninger om den grad af adgang, som underleverandører har til personoplysninger eller på anden måde følsomme oplysninger eller systemer, som vedrører de IKT-tjenester, som leveres til finansielle enheder — Oplysninger om de steder, hvorfra underleverandørernes tjenester leveres, og om de foranstaltninger, der er truffet for at mindske de risici, som hidrører fra tjenester, der leveres uden for Unionen.
Forvaltning af og tilsyn med underentreprise	— En beskrivelse af den kontraktlige ramme og den forvaltningsramme, der er indført for at forvalte underentrepriseforhold, herunder klausuler, som begrænser anvendelsen af følsomme data — En redegørelse for processerne vedrørende udvælgelse, ansættelse og overvågning af underleverandører — Oversigt over resultatindikatorer, mål og aftaler vedrørende serviceniveau og centrale resultatindikatorer, som anvendes til at vurdere underleverandørers resultater og overvågning af pålidelighed
Risikostyring og overholdelse	— Vurdering af underleverandørens risikoprofiler og potentielle indvirkning på de IKT-tjenester, der leveres til finansielle enheder — Redegørelse for de foranstaltninger til mindskelse af risici, som er gennemført for at imødegå risici forbundet med underentreprise — Nærmere oplysninger om underleverandørens overholdelse af relevante regler, herunder vedrørende databeskyttelse og industristandarder

Oplysningskategori	Elementer af centrale oplysninger
Planer for driftsstabilitet og beredskabsplaner	— Oversigt over underleverandørens planer for driftsstabiliteten samt indsats- og genopretningsplaner — En beskrivelse af de indførte ordninger, som skal sikre driftsstabilitet i tilfælde af afbrydelser eller opsigelse fra underleverandørens side — Hyppigheden af underleverandørens test af planerne for driftsstabilitet samt indsats- og genopretningsplanerne, datoer for de seneste test i løbet af de foregående tre år og præcisering heraf, hvis den kritiske tredjepartsudbyder af IKT-tjenester har været involveret i disse test
Indberetning	— En beskrivelse af indberetningsmekanismerne og indberetningsfrekvensen mellem den kritiske tredjepartsudbyder af IKT-tjenester og dens underleverandører
Udbedring og styring af hændelser	— En sammenfatning af procedurerne for imødegåelse af hændelser, brud eller manglende overholdelse, som er forbundet med underleverandører
Certificeringer og revisioner	— Oplysninger om certificeringer, uafhængige revisioner eller vurderinger af underleverandører for at validere deres sikkerhedskontroller, kvalitetsstandarder eller overholdelse af forskrifter — Dato for og hyppighed af revisionerne af underleverandørerne, som den kritiske tredjepartsudbyder af IKT-tjenester har foretaget