Europeiska unionens
officiella tidning

SV
L-serien

2025/295

13.2.2025

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2025/295

av den 24 oktober 2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska tillsynsstandarder som möjliggör genomförandet av tillsynsverksamhet

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 ([1]), särskilt artikel 41.2 andra stycket, och

av följande skäl:

(1) Genom det regelverk för digital operativ motståndskraft för finanssektorn som fastställs i förordning (EU) 2022/2554 införs en ram på unionsnivå för tillsyn över de tredjepartsleverantörer som tillhandahåller informations- och kommunikationsteknik (IKT) till finanssektorn och som har klassificerats som kritiska i enlighet med artikel 31 i den förordningen.

(2) En tredjepartsleverantör av IKT-tjänster som lämnar in en ansökan om frivillig begäran att bli klassificerad som kritisk bör till den mottagande europeiska tillsynsmyndigheten lämna all information som krävs för att styrka sin kritikalitet enligt de principer och kriterier som fastställs i förordning (EU) 2022/2554. Den information som ska ingå i en ansökan om frivillig begäran bör därför vara tillräckligt utförlig och fullständig för att möjliggöra en säker och fullständig bedömning av kritikaliteten i enlighet med artikel 31.11 i den förordningen. Den berörda europeiska tillsynsmyndigheten bör avvisa ofullständiga ansökningar och begära in de uppgifter som saknas.

(3) Den rättsliga identifieringen av tredjepartsleverantörer av IKT-tjänster som omfattas av dessa tekniska tillsynsstandarder bör anpassas till den id-kod som anges i den genomförandeförordning som kommissionen antagit i enlighet med artikel 28.9 i förordning (EU) 2022/2554.

(4) Den ledande tillsynsmyndigheten bör följa upp sina rekommendationer till kritiska tredjepartsleverantörer av IKT-tjänster genom att övervaka deras efterlevnad. För att säkerställa en effektiv och ändamålsenlig övervakning av de åtgärder eller avhjälpande åtgärder som har genomförts av kritiska tredjepartsleverantörer av IKT-tjänster med anledning av dessa rekommendationer bör den ledande tillsynsmyndigheten kunna begära in de rapporter som avses i artikel 35.1 c i förordning (EU) 2022/2554 i form av läges- och slutrapporter.

(5) För den bedömning som anges i artikel 42.1 i förordning (EU) 2022/2554, enligt vilken den ledande tillsynsmyndigheten är skyldig att ta ställning till om den förklaring som lämnats av den kritiska tredjepartsleverantören av IKT-tjänster är tillräcklig, bör underrättelsen från den kritiska tredjepartsleverantören av IKT-tjänster till den ledande tillsynsmyndigheten om att den har för avsikt att följa mottagna rekommendationer kompletteras med en beskrivning av de åtgärder och avhjälpande åtgärder som har vidtagits för att minska de risker som beskrivs i rekommendationerna, tillsammans med deras respektive tidsfrister. En sådan förklaring bör ha formen av en åtgärdsplan.

(6) Eftersom den ledande tillsynsmyndigheten förväntas bedöma underleverantörsavtal som ingåtts av den kritiska tredjepartsleverantören av IKT-tjänster måste en mall utformas för tillhandahållandet av information om dessa avtal. Mallen bör ta hänsyn till att strukturen hos kritiska tredjepartsleverantörer av IKT-tjänster skiljer sig från den hos finansiella entiteter.

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

(7) När den ledande tillsynsmyndigheten har utfärdat rekommendationer till en kritisk tredjepartsleverantör av IKT-tjänster och behöriga myndigheter har informerat relevanta finansiella entiteter om de risker som identifieras i rekommendationerna bör den ledande tillsynsmyndigheten övervaka och bedöma de åtgärder och avhjälpande åtgärder som genomförs av den kritiska tredjepartsleverantören av IKT-tjänster för att följa rekommendationerna. Behöriga myndigheter bör övervaka och bedöma i vilken utsträckning finansiella entiteter är exponerade för de risker som identifieras i dessa rekommendationer. För att under utförandet av sina respektive uppgifter säkerställa lika konkurrensvillkor, i synnerhet när de risker som identifieras i rekommendationerna är allvarliga och gemensamma för ett stort antal finansiella entiteter i flera medlemsstater, bör behöriga myndigheter och den ledande tillsynsmyndigheten delge varandra alla relevanta resultat som är nödvändiga för utförandet av deras respektive uppgifter. Syftet med detta utbyte av information är att säkerställa att den ledande tillsynsmyndighetens återkoppling till den kritiska tredjepartsleverantören av IKT-tjänster gällande de åtgärder och avhjälpande åtgärder som genomförs av den sistnämnda tar hänsyn till effekten på finansiella entiteters risker och att behöriga myndigheters tillsynsverksamhet beaktar den ledande tillsynsmyndighetens bedömning.

(8) För att möjliggöra ett effektivt och ändamålsenligt utbyte av information bör behöriga myndigheter som ett led i sin tillsynsverksamhet bedöma i vilken utsträckning finansiella entiteter som står under deras tillsyn är exponerade för de risker som identifieras i rekommendationerna. Denna bedömning bör vara proportionell och riskbaserad. Den ledande tillsynsmyndigheten bör be behöriga myndigheter att få ta del av resultaten av denna bedömning i fall där de risker som identifieras i rekommendationerna är allvarliga och gemensamma för ett stort antal finansiella entiteter i flera medlemsstater. För att utnyttja behöriga myndigheters resurser på bästa sätt bör den ledande tillsynsmyndigheten, när den begär att få ta del av resultaten av denna bedömning, alltid ta hänsyn till att syftet är att bedöma de åtgärder och avhjälpande åtgärder som genomförts av kritiska tredjepartsleverantörer av IKT-tjänster.

(9) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([2]) och avgav ett yttrande den 22 juli 2024.

(10) Denna förordning grundar sig på det förslag till tekniska tillsynsstandarder som de europeiska tillsynsmyndigheterna har överlämnat till kommissionen.

(11) De europeiska tillsynsmyndigheternas gemensamma kommitté har genomfört öppna offentliga samråd om det förslag till tekniska tillsynsstandarder som denna förordning grundas på, gjort en analys av potentiella kostnader och fördelar samt begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([3]), den intressentgrupp för försäkring och återförsäkring och den intressentgrupp för tjänstepensioner som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([4]), samt den intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([5]).

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

([3]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Information som tredjepartsleverantörer av IKT-tjänster ska lämna i en ansökan om att bli klassificerad som kritisk

1. Tredjepartsleverantören av informations- och kommunikationsteknik (IKT) ska lämna följande information i sin motiverade ansökan om frivillig begäran enligt artikel 31.11 i förordning (EU) 2022/2554 om att bli klassificerad som kritisk i enlighet med artikel 31.1 a i förordning (EU) 2022/2554:

a) Den juridiska personens namn.

b) Identifieringskod för juridiska personer (LEI-kod).

c) Namn på kontaktperson och kontaktuppgifter för den kritiska tredjepartsleverantören av IKT-tjänster.

d) Land där den juridiska personen har sitt säte.

e) Beskrivning av företagsstruktur med uppgift om åtminstone moderföretag och andra närstående företag som tillhandahåller IKT-tjänster till finansiella entiteter i EU. Denna information ska i tillämpliga fall omfatta följande:

   i) De juridiska personernas namn.

   ii) Identifieringskod för juridiska personer (LEI-kod).

   iii) Land där den juridiska personen har sitt säte.

f) Beräknad marknadsandel för tredjelandsleverantören av IKT-tjänster i unionens finanssektor och beräknad marknadsandel per typ av finansiell entitet som anges i artikel 2.1 i förordning (EU) 2022/2554 det år ansökan om att bli klassificerad som kritisk lämnas in och året före denna ansökan.

g) Beskrivning av varje IKT-tjänst som tillhandahålls finansiella entiteter i unionen, inbegripet

   i) beskrivning av typen av verksamhet och typen av IKT-tjänster som tillhandahålls finansiella entiteter,

   ii) om tillgänglig, en förteckning över de funktioner hos finansiella entiteter som stöds av de tillhandahållna IKT-tjänsterna,

   iii) om tillgänglig, information om huruvida de IKT-tjänster som tillhandahålls finansiella entiteter stöder kritiska eller viktiga funktioner.

h) Om tillgänglig, en förteckning över finansiella entiteter som använder de IKT-tjänster som tillhandahålls av tredjepartsleverantören av IKT-tjänster, inbegripet följande information för var och en av dessa finansiella entiteter:

   i) Den juridiska personens namn.

   ii) Identifieringskod för juridiska personer (LEI-kod), om tredjepartsleverantören av IKT-tjänster känner till denna.

   iii) Typ av finansiell entitet enligt artikel 2.1 i förordning (EU) 2022/2554.

   iv) Geografisk plats från vilken IKT-tjänsterna tillhandahålls den specifika juridiska personen.

i) Om tillgänglig, en förteckning över de kritiska tredjepartsleverantörer av IKT-tjänster som ingår i den senaste förteckning över sådana leverantörer som de europeiska tillsynsmyndigheterna har offentliggjort i enlighet med artikel 31.9 i förordning (EU) 2022/2554 och som är beroende av de tjänster som tillhandahålls av sökanden.

j) En självbedömning av följande:

   i) Graden av utbytbarhet för varje IKT-tjänst som tillhandahålls av sökanden med beaktande av följande:

      — Marknadsandelen för tredjepartsleverantören av IKT-tjänster inom unionens finanssektor.

— Antalet kända relevanta konkurrenter per typ av IKT-tjänst eller grupp av IKT-tjänster.

— Närmare beskrivning av de IKT-tjänster som erbjuds, till exempel eventuell proprietär teknik, eller av organisationen hos, eller den verksamhet som bedrivs av, tredjepartsleverantören av IKT-tjänster.

ii) Kännedom om alternativa tredjepartsleverantörer som kan tillhandahålla samma IKT-tjänster som den tredjepartsleverantör av IKT-tjänster som lämnar in ansökan.

k) Information om en framtida affärsstrategi för tillhandahållandet av IKT-tjänster och infrastruktur för finansiella entiteter i unionen, inbegripet eventuella planerade förändringar i koncern- eller ledningsstrukturen och inträde på nya marknader eller upptagande av ny verksamhet.

l) Identifiering av de underleverantörer till den tredjepartsleverantör av IKT-tjänster som har klassificerats som kritiska tredjepartsleverantörer av IKT-tjänster.

m) Andra skäl som är relevanta för att tredjepartsleverantören av IKT-tjänster ska bli klassificerad som kritisk.

2. Om tredjepartsleverantören av IKT-tjänster ingår i en koncern ska informationen i punkt 1 lämnas avseende IKT-tjänster som tillhandahålls av koncernen som helhet.

Artikel 2

Innehåll, struktur och format avseende den information som kritiska tredjepartsleverantörer av IKT-tjänster ska lämna in, offentliggöra eller rapportera

1. Kritiska tredjepartsleverantörer av IKT-tjänster ska på begäran ge den ledande tillsynsmyndigheten all information som denna myndighet behöver för att kunna fullgöra sina tillsynsuppgifter i enlighet med kraven i förordning (EU) 2022/2554.

2. Den information som avses i punkt 1 omfattar bland annat följande:

a) Information om avtal och kopior av avtalshandlingar mellan

i) den kritiska tredjepartsleverantören av IKT-tjänster och de finansiella entiteter som anges i artikel 2.1 i förordning (EU) 2022/2554,

ii) den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer i syfte att visa den tekniska värdekedjan för de IKT-tjänster som tillhandahålls finansiella entiteter i unionen.

b) Information om organisations- och koncernstruktur hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet identifiering av alla enheter som tillhör samma koncern och som direkt eller indirekt tillhandahåller IKT-tjänster till finansiella entiteter i unionen.

c) Information om de största aktieägarna, inbegripet deras struktur och geografiska spridning, om de

i) ensamma eller tillsammans med sina anknutna enheter, innehar 25 % eller mer av kapitalet eller rösterna i den kritiska tredjepartsleverantören av IKT-tjänster,

ii) har rätt att utse eller avsätta en majoritet av ledamöterna i förvaltnings-, lednings- eller tillsynsorganet för den kritiska tredjepartsleverantören av IKT-tjänster,

iii) enligt ett avtal kontrollerar majoriteten av aktieägarnas eller medlemmarnas rösträtter i den kritiska tredjepartsleverantören av IKT-tjänster.

d) Information om den marknadsandel som den kritiska tredjepartsleverantören av IKT-tjänster har per typ av tjänst på de relevanta marknader där den är verksam.

e) Information om interna styrformer hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet regler för ansvar och ansvarsskyldighet.

f) Mötesprotokoll från ledningsorganet för den kritiska tredjepartsleverantören av IKT-tjänster och andra relevanta interna kommittéer som på något sätt behandlar verksamhet och risker avseende tredjepartsleverantörers IKT-tjänster som stöder funktioner hos finansiella entiteter inom unionen.

g) Information om IKT-säkerheten hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet relevanta strategier, mål, riktlinjer, förfaranden, protokoll, processer, kontrollåtgärder för att skydda känsliga uppgifter, åtkomstkontroller, krypteringsmetoder, incidenthanteringsplaner och information om efterlevnad av alla relevanta bestämmelser och i förekommande fall nationella och internationella standarder.

h) Information om tekniska och organisatoriska åtgärder för att säkerställa dataskydd och datasekretess för bland annat personuppgifter och andra uppgifter än personuppgifter, om genomförda kontrollåtgärder för att skydda känsliga uppgifter, om åtkomst, kontroller av krypteringsmetoder och plan för hantering av dataintrång, samt – när tredjepartsleverantören av IKT-tjänster i fråga om behandling av personuppgifter omfattas av lagstiftning i tredjeländer, inbegripet att tredjeländers myndigheter begär åtkomst – en förteckning över dessa länder och tillämplig lagstiftning.

i) Information om de mekanismer som den kritiska tredjepartsleverantören av IKT-tjänster erbjuder finansiella entiteter i unionen för dataportabilitet, tillämpningsportabilitet och interoperabilitet.

j) Information om lokalisering av datacenter och IKT-produktionscenter som används för att tillhandahålla tjänster till de finansiella entiteterna, inbegripet en förteckning över alla relevanta lokaler och anläggningar som tillhör den kritiska tredjepartsleverantören av IKT-tjänster, även utanför unionen.

k) Information i fall där den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster från tredjeländer, inbegripet information om relevanta rättsliga bestämmelser som är tillämpliga på personuppgifter och andra uppgifter än personuppgifter som behandlas av tredjepartsleverantören av IKT-tjänster.

l) Information om åtgärder som vidtagits för att hantera risker som uppstår till följd av att den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer från tredjeländer tillhandahåller IKT-tjänster.

m) Information om riskhanteringsram och ram för incidenthantering, inbegripet riktlinjer, förfaranden, verktyg, mekanismer och styrformer för den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer, en förteckning över och en beskrivning av allvarliga incidenter med direkt eller indirekt inverkan på finansiella entiteter inom unionen, samt relevanta uppgifter för att fastställa incidentens betydelse för finansiella entiteter och bedöma eventuella gränsöverskridande konsekvenser.

n) Information om ram för förändringshantering, inbegripet riktlinjer, förfaranden och kontroller för den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer.

o) Information om övergripande åtgärds- och återställningsram hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet kontinuitetsplaner och arrangemang och förfaranden i samband med dessa, policy för programvaruutvecklingens livscykel, åtgärds- och återställningsplaner och arrangemang och förfaranden i samband med dessa samt strategier och förfaranden för säkerhetskopiering.

p) Information om prestandaövervakning, säkerhetsövervakning och incidentspårning samt information om rapporteringsmekanismer när det gäller tjänstekvalitet, incidenter och efterlevnad av överenskomna servicenivåavtal och servicenivåmål eller liknande arrangemang mellan kritiska tredjepartsleverantörer av IKT-tjänster och finansiella entiteter i unionen.

q) Information om ram för tredjepartsförvaltning av IKT-tjänster hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet strategier, riktlinjer, förfaranden, processer och kontroller, inbegripet uppgifter om den *due diligence*-granskning och riskbedömning som den kritiska tredjepartsleverantören av IKT-tjänster gör av underleverantörer innan den ingår ett avtal med dem och för att övervaka avtalsförhållandet, vilka ska beakta alla relevanta IKT-risker och motpartsrisker.

r) Utdrag från övervaknings- och skanningssystem hos den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer som omfattar, men inte är begränsade till, nätverksövervakning, serverövervakning, applikationsövervakning, säkerhetsövervakning, sårbarhetsanalyser, logghantering, prestandaövervakning, incidenthantering och mätningar mot mål avseende tillförlitlighet, till exempel servicenivåmål.

s) Utdrag från produktions-, förproduktions- och testsystem eller applikationer som den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer använder för att direkt eller indirekt tillhandahålla tjänster till finansiella entiteter i unionen.

t) Regelefterlevnadsrapporter och tillgängliga revisionsrapporter, samt alla relevanta revisionsiakttagelser, inbegripet revisioner som utförs av nationella myndigheter i och utanför unionen om samarbetsavtal med de relevanta myndigheterna föreskriver ett sådant informationsutbyte, eller certifieringar av den kritiska tredjepartsleverantören av IKT-tjänster eller dess underleverantörer, inbegripet rapporter från interna och externa revisorer, certifieringar eller bedömningar av överensstämmelse med branschspecifika standarder. Detta omfattar information om alla typer av tillgängliga oberoende tester av motståndskraften hos IKT-systemen hos den kritiska tredjepartsleverantören av IKT-tjänster, inbegripet alla typer av hotbildsstyrd penetrationstestning som utförs av tredjepartsleverantören av IKT-tjänster.

u) Information om eventuella bedömningar som utförts av den kritiska tredjepartsleverantören av IKT-tjänster på dess begäran eller för dess räkning gällande lämpligheten och integriteten hos personer som innehar nyckelpositioner hos den kritiska tredjepartsleverantören av IKT-tjänster.

v) Information om eventuell åtgärdsplan för att följa rekommendationer i enlighet med artikel 3 och relevant relaterad information för att bekräfta att avhjälpande åtgärder har genomförts.

w) Information om tillgängliga utbildningsprogram för anställda och program för säkerhetsmedvetenhet, inbegripet, i förekommande fall, information om investeringar, resurser och metoder hos den kritiska tredjepartsleverantören av IKT-tjänster för att utbilda personalen i hantering av känsliga finansiella uppgifter och upprätthållande av en hög säkerhetsnivå.

x) Information om den verksamhet som bedrivs av den kritiska tredjepartsleverantören av IKT-tjänster och finansiella rapporter, inbegripet information om budget och resurser som rör IKT och säkerhet.

Artikel 3

Information från kritiska tredjepartsleverantörer av IKT-tjänster efter utfärdandet av rekommendationer

1. Den kritiska tredjepartsleverantören av IKT-tjänster ska tillhandahålla den ledande tillsynsmyndigheten en rapport med en åtgärdsplan avseende de rekommendationer och avhjälpande åtgärder som den kritiska tredjepartsleverantören av IKT-tjänster planerar att genomföra för att minska de risker som identifieras i de rekommendationer som avses i artikel 35.1 d i förordning (EU) 2022/2254. Rapporten ska vara förenlig med den tidsfrist som fastställts av den ledande tillsynsmyndigheten för varje rekommendation.

2. För att göra det möjligt att övervaka de åtgärder eller avhjälpande åtgärder som den kritiska tredjepartsleverantören av IKT-tjänster har genomfört med anledning av de rekommendationer som den mottagit ska den kritiska tredjepartsleverantören av IKT-tjänster på begäran låta den ledande tillsynsmyndigheten ta del av följande:

a) Lägesrapporter tillsammans med styrkande dokumentation som anger vilka framsteg som gjorts i genomförandet av de insatser och åtgärder som beskrivs i den rapport som den kritiska tredjepartsleverantören av IKT-produkter har lämnat till den ledande tillsynsmyndigheten inom den av denna myndighet fastställda tidsfristen.

b) Slutrapporter tillsammans med styrkande dokumentation som anger vilka åtgärder eller avhjälpande åtgärder som har genomförts av den kritiska tredjepartsleverantören av IKT-tjänster för att minska de risker som identifieras i de mottagna rekommendationerna.

Artikel 4

Struktur och format för den information som ska lämnas av kritiska tredjepartsleverantörer av IKT-tjänster

1. Den kritiska tredjepartsleverantören av IKT-tjänster ska lämna den begärda informationen till den ledande tillsynsmyndigheten genom de särskilda säkra elektroniska kanaler, och i den form, som anges av den ledande tillsynsmyndigheten.

2. När de kritiska tredjepartsleverantörerna av IKT-tjänster lämnar informationen till den ledande tillsynsmyndigheten ska de

a) följa den struktur som den ledande tillsynsmyndigheten anger i sin begäran om information,

b) tydligt ange var i den inlämnade dokumentationen man hittar den relevanta informationen.

3. Information som lämnas, offentliggörs eller rapporteras till den ledande tillsynsmyndigheten av den kritiska tredjepartsleverantören av IKT-tjänster ska vara på ett språk som är brukligt i internationella finanskretsar.

Artikel 5

Mall för lämnande av information om underleverantörsavtal

En kritisk tredjepartsleverantör av IKT-tjänster som är skyldig att lämna information om underleverantörsavtal ska lämna denna information till den ledande tillsynsmyndigheten i enlighet med mallen i bilagan.

Artikel 6

Behöriga myndigheters bedömning av de risker som identifieras i den ledande tillsynsmyndighetens rekommendationer

1. Den behöriga myndigheten ska i enlighet med proportionalitetsprincipen och som ett led i sin tillsyn över finansiella entiteter bedöma effekterna på finansiella entiteter av de åtgärder som den kritiska tredjepartsleverantören av IKT-tjänster har vidtagit med anledning av den ledande tillsynsmyndighetens rekommendationer.

2. Den behöriga myndigheten ska i den bedömning som avses i punkt 1 ta hänsyn till följande:

a) Om de korrigerande och avhjälpande åtgärder som finansiella entiteter genomfört för att minska de risker som identifieras i rekommendationerna är tillräckliga och konsekventa.

b) Den ledande tillsynsmyndighetens bedömning av om den kritiska tredjepartsleverantören av IKT-tjänster har rättat sig efter de åtgärder och insatser som ingår i rapporten i fall där detta påverkar exponeringen för de risker som identifieras i rekommendationerna för finansiella entiteter inom deras ansvarsområde.

c) Synpunkter från andra behöriga myndigheter till följd av samråd i enlighet med artikel 42.5 i förordning (EU) 2022/2554.

d) Om den ledande tillsynsmyndigheten har ansett att de åtgärder och avhjälpande åtgärder som vidtagits av den kritiska tredjepartsleverantören av IKT-tjänster är tillräckliga för att minska exponeringen för de risker som identifieras i rekommendationerna för finansiella entiteter inom deras ansvarsområde.

3. Den behöriga myndigheten ska på den ledande tillsynsmyndighetens begäran och inom rimlig tid överlämna resultaten av den bedömning som avses i punkt 1. När den ledande tillsynsmyndigheten begär att få tillgång till resultaten av denna bedömning ska den beakta proportionalitetsprincipen och omfattningen av de risker som identifieras i rekommendationerna, inbegripet de gränsöverskridande effekterna av dessa risker när de påverkar finansiella entiteter som är verksamma i mer än en medlemsstat.

4. Den behöriga myndigheten ska i relevanta fall begära att de finansiella entiteterna lämnar all information som krävs för att utföra den bedömning som avses i punkt 1.

Artikel 7

Ikraftträdande

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

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

Utfärdad i Bryssel den 24 oktober 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

MALL FÖR UTBYTE AV INFORMATION OM UNDERLEVERANTÖRSAVTAL

Informationskategori	Grundläggande uppgifter
Allmän information	— Namn på den kritiska tredjepartsleverantören av IKT-tjänster. — Id-kod för den kritiska tredjepartsleverantören av IKT-tjänster. — Namn på kontaktperson och kontaktuppgifter för den kritiska tredjepartsleverantören av IKT-tjänster. — Datum för inlämning av mallen.
Översikt över underleverantörsavtal	— Kartläggning av underleverantörsavtal med en kortfattad beskrivning av syftet med, och omfattningen av, förhållandet till underleverantörer (inbegripet en indikation om hur kritiska eller viktiga underleverantörsavtalen är för den kritiska tredjepartsleverantören av IKT-tjänster). — Specifikation och beskrivning av de typer av IKT-tjänster som lagts ut på underleverantörer och deras betydelse för de IKT-tjänster som tillhandahålls finansiella entiteter, i linje med de tekniska genomförandestandarder som antagits i enlighet med artikel 28.9 i förordning (EU) 2022/2554. — Vid specificering av typerna av IKT-tjänster, hänvisa till förteckningen i bilaga IV till de tekniska genomförandestandarder som antagits i enlighet med artikel 28.9 i förordning (EU) 2022/2554.
Information om underleverantörer	— Namn och uppgifter om juridisk person (inbegripet id-kod) för varje underleverantör. — Kontaktuppgifter för de personer som ansvarar för varje enskilt underleverantörsförhållande i ledningsstrukturen hos den kritiska tredjepartsleverantören av IKT-tjänster. — Översikt över varje underleverantörs sakkunskap, erfarenhet och kvalifikationer när det gäller de utkontrakterade IKT-tjänsterna.
Beskrivning av tjänster som tillhandahålls av underleverantörer	— Närmare beskrivning av de specifika IKT-tjänster som tillhandahålls av varje underleverantör. — Fördelning av ansvarsområden och uppgifter som lagts ut på underleverantörer med en närmare beskrivning av de olika rollerna i olika skeden av IKT-processerna. — Information om underleverantörernas tillgång till personuppgifter eller andra känsliga uppgifter eller system i samband med de IKT-tjänster som de tillhandahåller finansiella entiteter. — Information om de platser från vilka underleverantörerna tillhandahåller sina tjänster och om de åtgärder som vidtagits för att hantera risker i samband med tjänster som tillhandahålls utanför unionen.
Styrning och övervakning av utkontraktering	— Beskrivning av avtals- och styrningsrelaterade ramverk för att hantera underleverantörsförhållanden, inbegripet klausuler som begränsar användningen av känsliga uppgifter. — Redogörelse för processer för val, anlitande och övervakning av underleverantörer. — Översikt över resultatmått, servicenivåmål och avtal, samt nyckelprestationsindikatorer som används för att bedöma underleverantörernas prestanda- och tillförlitlighetsövervakning.
Riskhantering och regelefterlevnad	— Bedömning av underleverantörens riskprofiler och potentiell inverkan på de IKT-tjänster som tillhandahålls finansiella entiteter — Redogörelse för riskreducerande åtgärder som vidtas för att hantera risker knutna till underleverantörsavtal — Uppgifter om underleverantörens efterlevnad av relevanta regler om bland annat dataskydd och branschstandarder

Informationskategori	Grundläggande uppgifter
Kontinuitets- och beredskapsplanering	— Översikt över underleverantörens kontinuitetsplan och åtgärds- och återhämtningsplan — Beskrivning av de arrangemang som införts för att säkerställa tjänstekontinuitet i händelse av avbrott eller uppsägning från underleverantörens sida — Hur ofta underleverantörernas kontinuitetsplaner och åtgärds- och återhämtningsplaner testas, datum för tester under de senaste tre åren och uppgift om den kritiska tredjepartsleverantören av IKT-tjänster har deltagit i dessa tester
Rapportering	— Beskrivning av rapporteringsmekanismer och rapporteringsfrekvens mellan den kritiska tredjepartsleverantören av IKT-tjänster och dess underleverantörer
Avhjälpande åtgärder och incidenthantering	— Beskrivning av förfaranden för att hantera underleverantörsrelaterade incidenter, överträdelser eller bristande regelefterlevnad
Certifiering och revision	— Information om certifieringar, oberoende revisioner eller bedömningar som utförs gällande underleverantörer för att validera deras säkerhetskontroller, kvalitetsstandarder eller regelefterlevnad — Datum och frekvens för de revisioner av underleverantörer som utförts av den kritiska tredjepartsleverantören av IKT-tjänster