Europeiska unionens
officiella tidning

SV
L-serien

2024/1773

25.6.2024

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2024/1773

av den 13 mars 2024

om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar det detaljerade innehållet i riktlinjerna för kontraktsmässiga arrangemang om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster

(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 28.10 tredje stycket, och

av följande skäl:

(1) Den ram för digital operativ motståndskraft för finanssektorn som inrättats genom förordning (EU) 2022/2554 kräver att finansiella entiteter fastställer vissa nyckelprinciper för att hantera IKT-tredjepartsrisker, vilka är av särskild betydelse när finansiella entiteter anlitar tredjepartsleverantörer av IKT-tjänster för att stödja sina kritiska eller viktiga funktioner.

(2) Finansiella entiteter ska inom sin IKT-riskhanteringsram anta och regelbundet se över en strategi för IKT-tredjepartsrisker. Enligt artikel 28.2 i förordning (EU) 2022/2554 ska denna strategi omfatta riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster. De ska tillämpas individuellt och, i förekommande fall, på undergrupps- och gruppnivå.

(3) Finansiella entiteter varierar mycket i storlek, struktur och intern organisation och i arten och komplexiteten av deras verksamhet och insatser. Det är nödvändigt att ta hänsyn till denna mångfald och samtidigt införa vissa grundläggande lagstadgade krav som är lämpliga för alla finansiella entiteter vid utarbetandet av riktlinjerna för kontraktsmässiga arrangemang om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner som tillhandahålls av tredjepartsleverantörer av IKT-tjänster (*riktlinjerna*), och att säkerställa att dessa krav tillämpas på ett proportionellt sätt.

(4) Om finansiella entiteter ingår i en koncern, bör det moderföretag som ansvarar för att upprätta finansiella rapporter på undergrupps- och gruppnivå därför säkerställa att riktlinjerna tillämpas på ett konsekvent och sammanhängande sätt inom koncernen.

(5) Vid tillämpningen av riktlinjerna bör koncerninterna IKT-tjänsteleverantörer, inklusive de som helt eller kollektivt ägs av finansiella entiteter som tillhör samma institutionella skyddssystem, betraktas som tredjepartsleverantörer av IKT-tjänster. Riskerna för koncerninterna IKT-tjänsteleverantörer kan vara olika, men de krav som är tillämpliga på dem är desamma enligt förordning (EU) 2022/2554. På liknande sätt bör riktlinjerna gälla för underleverantörer som tillhandahåller IKT-tjänster som stöder kritiska eller viktiga funktioner eller väsentliga delar därav till tredjepartsleverantörer av IKT-tjänster, där det finns en kedja av tredjepartsleverantörer av IKT-tjänster.

(6) Ledningsorganets yttersta ansvar för att hantera en finansiell entitets IKT-risk är en övergripande princip som också är tillämplig på användningen av tredjepartsleverantörer av IKT-tjänster. Detta ansvar bör vidare omsättas i ledningsorganets kontinuerliga engagemang i kontroll och övervakning av IKT-riskhantering, inbegripet antagande och översyn, minst en gång per år, av riktlinjerna.

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

(7) För att säkerställa lämplig rapportering till ledningsorganet bör riktlinjerna tydligt specificera och identifiera det interna ansvaret för godkännande, förvaltning, kontroll och dokumentation av kontraktsmässiga arrangemang om användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster (*kontraktsmässiga arrangemang*), inbegripet de IKT-tjänster som tillhandahålls enligt kontraktsmässiga arrangemang som avses i artikel 28.1 a i förordning (EU) 2022/2554.

(8) För att ta hänsyn till alla möjliga risker som kan uppstå vid upphandling av IKT-tjänster som stöder kritiska eller viktiga funktioner, bör riktlinjernas struktur följa alla steg i varje huvudfas i livscykeln för kontraktsmässiga arrangemang med tredjepartsleverantörer.

(9) För att minska de identifierade riskerna bör riktlinjerna specificera planeringen av kontraktsmässiga arrangemang, inbegripet riskbedömning, due diligence och godkännandeprocessen för nya eller väsentliga ändringar av dessa kontraktsmässiga arrangemang. För att hantera de risker som kan uppstå innan ett avtal ingås med en tredjepartsleverantör av IKT-tjänster, bör riktlinjerna ange en lämplig och proportionell process för att välja och bedöma lämpligheten hos potentiella tredjepartsleverantörer av IKT-tjänster och kräva att den finansiella entiteten tar hänsyn till en icke uttömmande lista över faktorer som tredjepartsleverantörerna av IKT-tjänster bör ha inrättat. Förteckningen bör innehålla uppgifter om tjänsteleverantörernas företagsanseende, deras ekonomiska, mänskliga och tekniska resurser, deras informationssäkerhet, deras organisationsstruktur, inbegripet riskhantering, och deras interna kontroller.

(10) För att säkerställa en sund riskhantering i tillhandahållandet av IKT-tjänster som stöder kritiska eller viktiga funktioner från tredjepartsleverantörer av IKT-tjänster, bör riktlinjerna innehålla information om genomförande, övervakning och förvaltning av de kontraktsmässiga arrangemangen, inklusive på grupp- eller undergruppsnivå, där så är tillämpligt. Detta inbegriper krav på avtalsklausuler om ömsesidiga skyldigheter för de finansiella entiteterna och tredjepartsleverantörerna av IKT-tjänster, vilka bör fastställas skriftligen. För att säkerställa en effektiv tillsyn och främja motståndskraft vid förändringar i affärsmodellen eller affärsmiljön bör riktlinjerna säkerställa finansiella entiteters eller utsedda tredje parters och behöriga myndigheters rätt till inspektioner och tillgång till information och bör också ytterligare specificera exitstrategier och uppsägningsprocesser.

(11) I den utsträckning personuppgifter behandlas av tredjepartsleverantörer av IKT-tjänster påverkar dessa riktlinjer och eventuella kontraktsmässiga arrangemang inte utan bör komplettera skyldigheterna enligt Europaparlamentets och rådets förordning (EU) 2016/679 ([2]), såsom att ha ett skriftligt avtal på plats som beskriver behandlingen av personuppgifter, krav på att säkerställa säkerheten vid behandling av personuppgifter och fastställande av alla andra delar som krävs enligt den förordningen.

([2]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) De europeiska tillsynsmyndigheternas gemensamma kommitté, som avses i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([3]), i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([4]) och i artikel 54 i Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([5]) har genomfört öppna offentliga samråd om det förslag till tekniska standarder för tillsyn som den här förordningen grundar sig på, analyserat de potentiella kostnaderna och fördelarna med de föreslagna standarderna och begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i förordning (EU) nr 1093/2010, den intressentgrupp för försäkring och återförsäkring och den intressentgrupp för tjänstepensionsfonder som inrättats i enlighet med artikel 37 i förordning (EU) nr 1094/2010 samt den intressentgrupp för värdepapper och marknader som inrättats i enlighet med artikel 37 i förordning (EU) nr 1095/2010.

(13) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]) och avgav ett yttrande den 24 januari 2024,

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Allmän riskprofil och komplexitet

Riktlinjerna för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster (*riktlinjerna*) ska ta hänsyn till finansiella entiteters storlek och övergripande riskprofil samt karaktären på, omfattningen av och inslagen av ökad eller minskad komplexitet i deras tjänster, verksamhet och insatser, inbegripet aspekter som rör följande:

a) Den typ av IKT-tjänster som ingår i kontraktsmässiga arrangemang om användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster (*kontraktsmässiga arrangemang*) mellan finansiella entiteter och tredjepartsleverantörer av IKT-tjänster.

b) Platsen för tredjepartsleverantören av IKT-tjänster eller för moderföretaget.

c) Om de IKT-tjänster som stöder kritiska eller viktiga funktioner tillhandahålls av en tredjepartsleverantör av IKT-tjänster som är belägen i en medlemsstat eller i ett tredjeland, även med beaktande av den plats från vilken IKT-tjänsterna tillhandahålls och den plats där uppgifterna behandlas och lagras.

d) Beskaffenheten hos de uppgifter som delas med tredjepartsleverantören av IKT-tjänster.

e) Huruvida tredjepartsleverantören av IKT-tjänster tillhör samma koncern som den finansiella entitet till vilken tjänsterna tillhandahålls.

([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).

([6]) 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).

f) Användning av tredjepartsleverantörer av IKT-tjänster som är auktoriserade, registrerade eller föremål för tillsyn eller övervakning av en behörig myndighet i en medlemsstat eller som omfattas av tillsynsramen enligt kapitel V avsnitt II i förordning (EU) 2022/2554, och användning av tredjepartsleverantörer av IKT-tjänster som inte är det.

g) Användning av tredjepartsleverantörer av IKT-tjänster som är auktoriserade, registrerade eller föremål för tillsyn eller övervakning av en tillsynsmyndighet i ett tredjeland, och användning av tredjepartsleverantörer av IKT-tjänster som inte är det.

h) Huruvida tillhandahållandet av IKT-tjänster som stöder kritiska eller viktiga funktioner är koncentrerat till en enda tredjepartsleverantör av IKT-tjänster eller ett litet antal sådana tjänsteleverantörer.

i) Överlåtbarheten av IKT-tjänster som stöder kritiska eller viktiga funktioner till en annan tredjepartsleverantör av IKT-tjänster, även till följd av tekniskspecifika egenskaper.

j) Den potentiella inverkan av störningar i tillhandahållandet av IKT-tjänster som stöder kritiska eller viktiga funktioner på kontinuiteten i den finansiella entitetens verksamhet och på tillgången till dess tjänster.

Artikel 2

Koncerntillämpning

Om denna förordning är tillämplig på undergrupps- eller gruppnivå, ska det moderföretag som är ansvarigt för att tillhandahålla grupp- eller undergruppsbaserade finansiella rapporter för koncernen säkerställa att riktlinjerna genomförs konsekvent i alla finansiella entiteter som ingår i koncernen och är tillräckliga för en effektiv tillämpning av denna förordning på alla relevanta nivåer inom koncernen.

Artikel 3

Organisationsstyrning

1. Ledningsorganet ska se över riktlinjerna minst en gång om året och vid behov uppdatera dem. Ändringar av riktlinjerna ska genomföras i god tid och så snart det är möjligt inom ramen för de relevanta kontraktsmässiga arrangemangen. Den finansiella entiteten ska dokumentera den planerade tidsplanen för genomförandet.

2. I riktlinjerna ska det fastställas eller hänvisas till en metod för att fastställa vilka IKT-tjänster som stöder kritiska eller viktiga funktioner. I riktlinjerna ska också anges när denna bedömning ska genomföras och ses över.

3. I riktlinjerna ska det interna ansvaret för godkännande, förvaltning, kontroll och dokumentation av relevanta kontraktsmässiga arrangemang anges tydligt och det ska säkerställas att lämplig kompetens, erfarenhet och kunskap upprätthålls inom den finansiella entiteten för att effektivt övervaka de relevanta kontraktsmässiga arrangemangen, inbegripet de IKT-tjänster som tillhandahålls enligt dessa arrangemang.

4. Utan att det påverkar den finansiella entitetens slutliga ansvar att effektivt övervaka relevanta kontraktsmässiga arrangemang, ska riktlinjerna kräva att tredjepartsleverantören av IKT-tjänster bedöms ha tillräckliga resurser för att säkerställa att den finansiella entiteten uppfyller alla lagstadgade krav avseende de IKT-tjänster som stöder kritiska eller viktiga funktioner som tillhandahålls.

5. I riktlinjerna ska det tydligt anges vilken roll i eller vilken medlem av den högre ledningen som ansvarar för att övervaka de relevanta avtalsarrangemangen. Riktlinjerna ska ange hur den rollen i eller medlemmen av den högre ledningen ska samarbeta med kontrollfunktionerna och fastställas rapporteringsvägar till ledningsorganet, inbegripet vilken typ av information som ska rapporteras och vilka dokument som ska tillhandahållas. Det ska också anges hur ofta sådan rapportering ska ske.

6. Riktlinjerna ska säkerställa att de kontraktsmässiga arrangemangen är förenliga med följande:

a) Den IKT-riskhanteringsram som avses i artikel 6 i förordning (EU) 2022/2554.

b) De riktlinjer för informationssäkerhet som avses i artikel 9.4 i förordning (EU) 2022/2554.

c) Den IKT-kontinuitetspolicy som avses i artikel 11 i förordning (EU) 2022/2554.

d) De krav på incidentrapportering som anges i artikel 19 i förordning (EU) 2022/2554.

7. Riktlinjerna ska omfatta krav på att IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster är föremål för oberoende översyn och ingår i revisionsplanen.

8. I riktlinjerna ska det uttryckligen anges att de kontraktsmässiga arrangemangen

a) inte befriar den finansiella entiteten och dess ledningsorgan från deras lagstadgade skyldigheter och deras skyldigheter gentemot sina kunder,

b) inte hindrar en effektiv tillsyn över en finansiell entitet och inte strider mot några tillsynsrestriktioner för tjänster och verksamhet,

c) ska kräva att tredjepartsleverantörer av IKT-tjänster samarbetar med de behöriga myndigheterna,

d) ska kräva att den finansiella entiteten, dess revisorer och behöriga myndigheter har faktisk tillgång till uppgifter och lokaler som rör användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner.

Artikel 4

Huvudfaser i livscykeln för antagandet och användningen av kontraktsmässiga arrangemang

Riktlinjerna ska specificera kraven, inklusive reglerna, ansvarsområdena och processerna, för varje huvudfas i livscykeln för det kontraktsmässiga arrangemanget, som omfattar minst följande:

a) Ledningsorganets ansvar, inbegripet dess deltagande i beslutsprocessen om användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.

b) Planering av kontraktsmässiga arrangemang, inbegripet riskbedömning, due diligence enligt artiklarna 5 och 6 och godkännandeprocessen avseende nya eller väsentliga ändringar av kontraktsmässiga arrangemang enligt artikel 8.4.

c) Inblandning av affärsenheter, internkontroll och andra relevanta enheter med avseende på kontraktsmässiga arrangemang.

d) Genomförande, övervakning och förvaltning av de kontraktsmässiga arrangemang som avses i artiklarna 7, 8 och 9, inbegripet på grupp- och undergruppsnivå, i tillämpliga fall.

e) Dokumentation och registerhållning, med beaktande av de krav avseende informationsregistret som fastställs i artikel 28.3 i förordning (EU) 2022/2554.

f) Exitstrategier och uppsägningsprocesser enligt artikel 10.

Artikel 5

Förhandsbedömning av risker

1. Riktlinjerna ska omfatta krav på att den finansiella entitetens affärsbehov fastställs innan ett kontraktsmässigt arrangemang ingås.

2. Riktlinjerna ska omfatta krav på att en riskbedömning görs på finansiell entitetsnivå och, i tillämpliga fall, på grupp- och undergruppsnivå innan ett kontraktsmässigt arrangemang ingås.

Riskbedömningen ska beakta alla relevanta krav i förordning (EU) 2022/2554 och tillämplig sektorsspecifik unionslagstiftning. Den ska särskilt beakta hur tillhandahållandet av IKT-tjänster som stöder kritiska eller viktiga funktioner från tredjepartsleverantörer av IKT-tjänster påverkar den finansiella entiteten och alla de risker som är förknippade med tillhandahållandet av dessa IKT-tjänster som stöder kritiska eller viktiga funktioner från tredjepartsleverantörer av IKT-tjänster, inbegripet följande:

a) Operativa risker.

b) Rättsliga risker.

c) IKT-risker.

d) Anseenderisker.

e) Risker kopplade till skyddet av konfidentiella uppgifter eller personuppgifter.

f) Risker kopplade till tillgången till uppgifter.

g) Risker kopplade till den plats där uppgifterna behandlas och lagras.

h) Risker kopplade till den plats där tredjepartsleverantören av IKT-tjänster befinner sig.

i) IKT-koncentrationsrisker på entitetsnivå.

Artikel 6

Due diligence

1. Riktlinjerna ska fastställa en lämplig och proportionell process för att välja och bedöma de potentiella tredjepartsleverantörerna av IKT-tjänster med beaktande av huruvida tredjepartsleverantören av IKT-tjänster är en koncernintern IKT-tjänsteleverantör eller inte, och ska kräva att den finansiella entiteten, innan den ingår ett kontraktsmässigt arrangemang, bedömer huruvida tredjepartsleverantören av IKT-tjänster

a) har affärsmässigt anseende, tillräckliga förmågor, sakkunskap och tillräckliga ekonomiska, mänskliga och tekniska resurser, standarder för informationssäkerhet, lämplig organisationsstruktur, riskhantering och interna kontroller och, i tillämpliga fall, de tillstånd eller registreringar som krävs för att tillhandahålla IKT-tjänster som stöder den kritiska eller viktiga funktionen på ett tillförlitligt och professionellt sätt,

b) har förmåga att övervaka relevant teknisk utveckling och identifiera ledande metoder på IKT-säkerhetsområdet och genomföra dem när så är lämpligt för att ha en effektiv och sund ram för digital operativ motståndskraft,

c) använder eller avser att använda IKT-underleverantörer för att utföra IKT-tjänster som stöder kritiska eller viktiga funktioner eller väsentliga delar av dessa,

d) är belägen, eller behandlar eller lagrar uppgifterna i ett tredjeland och, om så är fallet, huruvida denna praxis påverkar nivån av operativa risker eller anseenderisker eller risken för att påverkas av restriktiva åtgärder, inbegripet embargon och sanktioner, som kan påverka tredjepartsleverantörens förmåga att tillhandahålla IKT-tjänsterna eller den finansiella entitetens förmåga att ta emot dessa IKT-tjänster,

e) samtycker till kontraktsmässiga arrangemang som säkerställer att det är möjligt att utföra revisioner hos tredjepartsleverantören av IKT-tjänster, även på plats, av den finansiella entiteten själv, utsedda tredje parter och behöriga myndigheter,

f) handlar på ett etiskt och socialt ansvarsfullt sätt, respekterar mänskliga rättigheter och barns rättigheter, inbegripet förbud mot barnarbete, respekterar tillämpliga principer om miljöskydd och säkerställer lämpliga arbetsvillkor.

2. Riktlinjerna ska specificera den erforderliga säkerhetsnivå när det gäller effektiviteten hos tredjepartsleverantörers riskhanteringsram för IKT-tjänster som stöder kritiska eller viktiga funktioner som ska tillhandahållas av en tredjepartsleverantör av IKT-tjänster. Riktlinjerna ska innehålla krav på att förfarandet för due diligence omfattar en bedömning av förekomsten av riskreducerande åtgärder och åtgärder för driftskontinuitet och av hur de säkerställs inom tredjepartsleverantören av IKT-tjänster.

3. Riktlinjerna ska fastställa förfarandet för due diligence vid val och bedömning av potentiella tredjepartsleverantörer av IKT-tjänster och ange vilka av följande faktorer som ska användas för den erforderliga försäkran om tredjepartsleverantörens prestanda:

a) Revisioner eller oberoende bedömningar som utförs av den finansiella entiteten själv eller för dess räkning,

b) Användning av oberoende revisionsrapporter på begäran av tredjepartsleverantören av IKT-tjänster.

c) Användning av revisionsrapporter från tredjepartsleverantörens internrevisionsfunktion.

d) Användning av lämpliga tredjepartscertifieringar.

e) Användning av annan relevant information som är tillgänglig för den finansiella entiteten eller annan information som tillhandahålls av tredjepartsleverantören av IKT-tjänster.

4. Finansiella entiteter ska säkerställa en lämplig säkerhetsnivå för tredjepartsleverantörens prestanda, med beaktande av de faktorer som anges i punkt 3 a–e. I förekommande fall ska fler än en av de delar som förtecknas i dessa punkter användas.

Artikel 7

Intressekonflikter

1. Riktlinjerna ska ange lämpliga åtgärder för att identifiera, förhindra och hantera faktiska eller potentiella intressekonflikter till följd av användning av tredjepartsleverantörer av IKT-tjänster som ska vidtas innan relevanta kontraktsmässiga arrangemang ingås och ska föreskriva en fortlöpande övervakning av sådana intressekonflikter.

2. Om IKT-tjänster som stöder kritiska eller viktiga funktioner tillhandahålls av koncerninterna IKT-tjänsteleverantörer ska det i riktlinjerna anges att beslut om villkoren för IKT-tjänsterna, inbegripet finansiella villkor, ska fattas på ett objektivt sätt.

Artikel 8

Avtalsklausuler

1. I riktlinjerna ska det anges att det relevanta kontraktsmässiga arrangemanget ska vara skriftligt och omfatta alla de delar som avses i artikel 30.2 och 30.3 i förordning (EU) 2022/2554. Riktlinjerna ska också innehålla uppgifter om de krav som avses i artikel 1.1 a i förordning (EU) 2022/2554 samt, i förekommande fall, annan relevant unionsrätt och nationell rätt.

2. I riktlinjerna ska det anges att de relevanta kontraktsmässiga arrangemangen ska omfatta den finansiella entitetens rätt att få tillgång till information, att utföra inspektioner och revisioner och att utföra IKT-tester. För detta ändamål ska riktlinjerna kräva att den finansiella entiteten använder följande metoder, utan att det påverkar den finansiella entitetens slutliga ansvar:

a) Sin egen internrevision eller en revision utförd av en utsedd tredje part.

b) I förekommande fall, gemensamma revisioner och gemensamma IKT-tester, inbegripet hotbildsstyrd penetrationstestning, som anordnas tillsammans med andra upphandlande finansiella entiteter eller företag som använder IKT-tjänster från samma tredjepartsleverantör och som utförs av dessa upphandlande finansiella entiteter eller företag eller av en tredje part som utsetts av dem.

c) I tillämpliga fall, tredjepartscertifieringar.

d) I tillämpliga fall, internrevisionsrapporter eller tredjepartsrevisionsrapporter som tillhandahållits av tredjepartsleverantören av IKT-tjänster.

3. Den finansiella entiteten ska över tid inte enbart förlita sig på certifieringar som avses i punkt 2 c eller revisionsrapporter som avses i punkt 2 d. Riktlinjerna ska endast tillåta användning av de metoder som avses i punkt 2 c och d om den finansiella entiteten

a) är nöjd med revisionsplanen från tredjepartsleverantören av IKT-tjänster för de relevanta kontraktsmässiga arrangemangen,

b) säkerställer att certifieringarnas eller revisionsrapporternas omfattning inbegriper de system och grundläggande kontroller som den har identifierat och säkerställer överensstämmelse med relevanta lagstadgade krav,

c) noggrant utvärderar innehållet i certifieringarna eller revisionsrapporterna och kontrollerar att rapporterna eller certifieringarna inte är föråldrade,

d) säkerställer att viktiga system och kontroller omfattas av framtida versioner av certifieringen eller revisionsrapporten,

e) är nöjd med den certifierande eller reviderande partens lämplighet,

f) är övertygat om att certifieringarna utfärdas och att revisionerna utförs mot allmänt erkända relevanta yrkesstandarder och inbegriper ett test av den operativa effektiviteten hos de grundläggande kontrollerna.

g) har avtalsenlig rätt att, med en frekvens som är rimlig och berättigad ur ett riskhanteringsperspektiv, begära ändringar av certifieringarnas eller revisionsrapporternas omfattning till andra relevanta system och kontroller,

h) har avtalsenlig rätt att utföra enskilda och gemensamma revisioner efter eget gottfinnande med avseende på de kontraktsmässiga arrangemangen och verkställa dessa rättigheter i linje med den överenskomna frekvensen.

4. Riktlinjerna ska säkerställa att väsentliga ändringar av det kontraktsmässiga arrangemanget formaliseras i en skriftlig handling som dateras och undertecknas av alla parter och ska specificera förnyelseförfarandet för de kontraktsmässiga arrangemangen.

Artikel 9

Övervakning av de kontraktsmässiga arrangemangen

1. Riktlinjerna ska omfatta krav på att de kontraktsmässiga arrangemangen specificerar åtgärder och nyckelindikatorer för att löpande övervaka prestandan hos tredjepartsleverantörer av IKT-tjänster, inklusive åtgärder för att övervaka efterlevnaden av krav avseende sekretess, tillgänglighet, integritet och äkthet för data och information, och att tredjepartsleverantörer av IKT-tjänster följer den finansiella entitetens relevanta riktlinjer och förfaranden. I riktlinjerna ska också anges vilka åtgärder som ska tillämpas när servicenivåavtal inte uppfylls, inklusive avtalsenliga påföljder när så är lämpligt.

2. I riktlinjerna ska anges hur den finansiella entiteten ska bedöma huruvida de tredjepartsleverantörer av IKT-tjänster som används för IKT-tjänster som stöder kritiska eller viktiga funktioner uppfyller lämpliga prestanda- och kvalitetsstandarder i linje med det kontraktsmässiga arrangemanget och den finansiella entitetens egna riktlinjer. Riktlinjerna ska särskilt säkerställa följande:

a) Att tredjepartsleverantörerna av IKT-tjänster lämnar lämpliga rapporter om sin verksamhet och sina tjänster till den finansiella entiteten, inklusive periodiska rapporter, incidentrapporter, rapporter om tillhandahållande av tjänster, rapporter om IKT-säkerhet och rapporter om kontinuitetsåtgärder och tester.

b) Att prestandan för tredjepartsleverantören av IKT-tjänster bedöms med hjälp av nyckelutförandeindikatorer, centrala kontrollindikatorer, revisioner, självcertifieringar och oberoende granskningar i linje med den finansiella entitetens IKT-riskhanteringsram.

c) Att den finansiella entiteten får annan relevant information från tredjepartsleverantörer av IKT-tjänster.

d) Att den finansiella entiteten i förekommande fall underrättas om IKT-relaterade incidenter och betalningsrelaterade operativa incidenter eller säkerhetsincidenter.

e) Att en oberoende översyn och revision genomförs för att kontrollera efterlevnaden av lagstadgade krav och riktlinjer.

3. I riktlinjerna ska det anges att den bedömning som avses i punkt 2 ska dokumenteras och att dess resultat ska användas för att uppdatera den finansiella entitetens riskbedömning enligt artikel 6.

4. Riktlinjerna ska fastställa de lämpliga åtgärder som den finansiella entiteten ska vidta om den identifierar brister hos tredjepartsleverantörer av IKT-tjänster, inklusive IKT-relaterade incidenter och betalningsrelaterade operativa incidenter eller säkerhetsincidenter, i tillhandahållandet av IKT-tjänster som stöder kritiska eller viktiga funktioner eller i efterlevnaden av kontraktsmässiga arrangemang eller rättsliga krav. De ska också ange hur genomförandet av sådana åtgärder ska övervakas för att säkerställa att de efterlevs effektivt inom en fastställd tidsram, med beaktande av bristernas väsentlighet.

Artikel 10

Utträde från och uppsägning av de kontraktsmässiga arrangemangen

Riktlinjerna ska innehålla krav på en dokumenterad exitplan för varje kontraktsmässigt arrangemang och på regelbunden översyn och testning av den dokumenterade exitplanen. Vid upprättandet av exitplanen ska följande beaktas:

a) Oförutsedda och ihållande driftstopp i verksamheten.

b) Olämpligt eller misslyckat tillhandahållande av tjänster.

c) Oväntad uppsägning av det kontraktsmässiga arrangemanget.

Exitplanen ska vara realistisk, genomförbar, grundad på rimliga scenarier och rimliga antaganden och ska ha en planerad genomförandeplan som är förenlig med de villkor för utträde och uppsägning som fastställs i de kontraktsmässiga arrangemangen.

Artikel 11

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 13 mars 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande