2024/1773

25.6.2024

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2024/1773

af 13. marts 2024

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 for så vidt angår reguleringsmæssige tekniske standarder, der præciserer det detaljerede indhold af politikken vedrørende de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester

(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 28, stk. 10, tredje afsnit, og

ud fra følgende betragtninger:

(1) I henhold til rammen for digital operationel modstandsdygtighed i den finansielle sektor, der er fastsat ved forordning (EU) 2022/2554, skal finansielle enheder fastsætte visse centrale principper for styring af IKT-tredjepartsrisici, som er af særlig betydning, når finansielle enheder samarbejder med tredjepartsudbydere af IKT-tjenester om at understøtte deres kritiske eller vigtige funktioner.

(2) Finansielle enheder skal som led i deres ramme for IKT-risikostyring vedtage og regelmæssigt gennemgå en strategi for IKT-tredjepartsrisiko. I overensstemmelse med artikel 28, stk. 2, i forordning (EU) 2022/2554 skal denne strategi omfatte en politik for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester. Den skal finde anvendelse på individuelt grundlag og, hvis det er relevant, på delkonsolideret og konsolideret grundlag.

(3) Finansielle enheder varierer meget med hensyn til størrelse, struktur og intern organisation og med hensyn til karakteren og kompleksiteten af deres aktiviteter og transaktioner. Det er nødvendigt at tage hensyn til denne mangfoldighed, samtidig med at der indføres visse grundlæggende forskriftsmæssige krav, som er hensigtsmæssige for alle finansielle enheder, når de udvikler politikken vedrørende de kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner (»politikken«), og at sikre, at disse krav anvendes på en måde, der står i rimeligt for hold til formålet.

(4) Hvis finansielle enheder tilhører en koncern, bør den modervirksomhed, der har ansvar for at fremlægge det konsoliderede eller delkonsoliderede koncernregnskab, derfor sikre, at politikken anvendes på en konsekvent og sammenhængende måde inden for koncernen.

(5) Ved anvendelse af politikken bør koncerninterne udbydere IKT-tjenester, herunder dem, der ejes fuldt ud eller i fællesskab af finansielle enheder inden for samme institutsikringsordning, betragtes som tredjepartsudbydere af IKT-tjenester. De risici, som koncerninterne udbydere IKT-tjenester udgør, kan være forskellige, men de krav, der gælder for dem, er de samme i henhold til forordning (EU) 2022/2554. På samme måde bør politikken finde anvendelse på underleverandører, der leverer IKT-tjenester, der understøtter kritiske eller vigtige funktioner eller væsentlige dele heraf til tredjepartsudbydere af IKT-tjenester, hvis der er tale om en kæde af tredjepartsudbydere af IKT-tjenester.

(6) Ledelsesorganets endelige ansvar for styringen af en finansiel enheds IKT-risiko er et overordnet princip, som også finder anvendelse på brugen af tredjepartsudbydere af IKT-tjenester. Dette ansvar bør yderligere omsættes i form af ledelsesorganets fortsatte engagement i kontrollen og overvågningen af IKT-risikostyring, herunder i vedtagelsen og gennemgangen af politikken, mindst én gang om året.

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

(7) For at sikre passende rapportering til ledelsesorganet bør politikken klart præcisere og identificere det interne ansvar for godkendelse, forvaltning, kontrol og dokumentation af kontraktlige ordninger for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester (»kontraktlige ordninger«), herunder de IKT-tjenester, der leveres i henhold til kontraktlige ordninger som omhandlet i artikel 28, stk. 1, litra a), i forordning (EU) 2022/2554.

(8) For at tage hensyn til alle mulige risici, der kan opstå, når der indgås kontrakter om IKT-tjenester, der understøtter kritiske eller vigtige funktioner, bør politikkens struktur følge alle trin i hver hovedfase af livscyklussen for kontraktlige ordninger med tredjepartsudbydere.

(9) For at afbøde de konstaterede risici bør politikken beskrive planlægningen af kontraktlige ordninger, herunder risikovurderingen, due diligence- og godkendelsesprocessen for nye eller væsentlige ændringer af disse kontraktlige ordninger. For at styre de risici, der kan opstå, inden der indgås en kontraktlig ordning med en tredjepartsudbyder af IKT-tjenester, bør politikken fastlægge en passende og forholdsmæssigt afstemt proces for udvælgelse og vurdering af egnetheden af potentielle tredjepartsudbydere af IKT-tjenester og indeholde krav om, at den finansielle enhed skal tage hensyn til en ikkeudtømmende liste over elementer, som tredjepartsudbyderne af IKT-tjenester bør have indført. Listen bør omfatte elementer vedrørende tjenesteudbydernes forretningsmæssige omdømme, deres finansielle, menneskelige og tekniske ressourcer, deres informationssikkerhed, deres organisatoriske struktur, herunder risikostyring, og deres interne kontrol.

(10) For at sikre en forsvarlig risikostyring i forbindelse med af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester, bør politikken indeholde oplysninger om gennemførelsen, overvågningen og forvaltningen af de kontraktlige ordninger, herunder på konsolideret og delkonsolideret grundlag, hvis det er relevant. Dette omfatter krav til kontraktbestemmelserne om gensidige forpligtelser for de finansielle enheder og tredjepartsudbyderne af IKT-tjenester, som bør fastsættes skriftligt. For at sikre et effektivt tilsyn og fremme modstandsdygtighed i tilfælde af ændringer i forretningsmodellen eller erhvervsklimaet bør politikken garantere de finansielle enheders eller udpegede tredjeparters og kompetente myndigheders ret til inspektioner og adgang til oplysninger, og den bør også yderligere præcisere exitstrategierne og opsigelsesprocesserne.

(11) I det omfang tredjepartsudbydere af IKT-tjenester behandler personoplysninger, gælder denne politik og eventuelle kontraktlige ordninger dog med forbehold af eller supplerer forpligtelserne i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([2]), f.eks. til at have en skriftlig kontrakt, der beskriver behandlingen af personoplysninger, krav om at garantere sikkerheden i forbindelse med behandling af personoplysninger og fastsætter alle andre elementer, der kræves i henhold til nævnte forordning.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Det Fælles Udvalg af Europæiske Tilsynsmyndigheder, jf. artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([3]), artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([4]) og artikel 54 i Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([5]), har afholdt åbne offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele ved de foreslåede standarder og anmodet om rådgivning fra interessentgruppen for banker, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1093/2010, interessentgruppen for forsikrings- og genforsikringsordninger og interessentgruppen for arbejdsmarkedspensionsordninger, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1094/2010, og interessentgruppen for værdipapirer og markeder, der er nedsat i henhold til artikel 37 i forordning (EU) nr. 1095/2010.

(13) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav en udtalelse den 24. januar 2024 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Overordnet risikoprofil og kompleksitet

Politikken for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester (»politikken«), skal tage hensyn til den finansielle enheds størrelse og overordnede risikoprofil og karakteren, omfanget og elementerne af øget eller reduceret kompleksitet af dens tjenester, aktiviteter og operationer, herunder elementer vedrørende:

a) typen af IKT-tjenester, der er omfattet af den kontraktlige ordning for brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester (»den kontraktlige ordning«), mellem den finansielle enhed og tredjepartsudbyderen af IKT-tjenester

b) det sted, hvor tredjepartsudbyderen af IKT-tjenester eller dennes moderselskabs er beliggende

c) om de IKT-tjenester, der understøtter kritiske eller vigtige funktioner, leveres af en tredjepartsudbyder af IKT-tjenester i en medlemsstat eller i et tredjeland, også under hensyntagen til det sted, hvorfra IKT-tjenesterne leveres, og det sted, hvor dataene behandles og lagres

d) arten af de data, der deles med tredjepartsudbyderen af IKT-tjenester

e) hvorvidt tredjepartsudbyderen af IKT-tjenester er del af samme koncern som den finansielle enhed, som tjenesterne leveres til

([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).

([6]) 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).

f) brugen af tredjepartsudbydere af IKT-tjenester, der er godkendt, registreret eller underlagt tilsyn eller overvågning, der udøves af en kompetent myndighed i en medlemsstat, eller som er underlagt tilsynsrammen i henhold til kapitel V, afdeling II, i forordning (EU) 2022/2554, og brugen af tredjepartsudbydere af IKT-tjenester, for hvilke ovennævnte forhold ikke gør sig gældende

g) brugen af tredjepartsudbydere af IKT-tjenester, der er godkendt, registreret eller underlagt tilsyn eller overvågning, der udøves af en tilsynsmyndighed i et tredjeland, og brugen af tredjepartsudbydere af IKT-tjenester, for hvilke ovennævnte forhold ikke gør sig gældende

h) hvorvidt leveringen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, hidrører fra én en enkelt tredjepartsudbyder af IKT-tjenester eller et lille antal af sådanne tjenesteudbydere

i) hvorvidt det er muligt at overføre de IKT-tjenester, der understøtter kritiske eller vigtige funktioner, til en anden tredjepartsudbyder af IKT-tjenester, herunder som følge af særlige teknologiske forhold

j) den potentielle indvirkning af forstyrrelser i leveringen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, på driftsstabiliteten af den finansielle enheds aktiviteter og på tilgængeligheden af dens tjenester.

Artikel 2

Anvendelse på koncernniveau

Hvis denne forordning finder anvendelse på delkonsolideret eller konsolideret niveau, sikrer den modervirksomhed, der har ansvar for at fremlægge det konsoliderede eller delkonsoliderede koncernregnskab, at politikken gennemføres konsekvent i alle finansielle enheder, der er en del af koncernen, og at den er tilstrækkelig til, at denne forordning kan finde effektiv anvendelse på alle relevante koncernniveauer.

Artikel 3

Ledelsesordninger

1. Ledelsesorganet gennemgår politikken mindst én gang om året og ajourfører den om nødvendigt. Ændringer af politikken gennemføres rettidigt og så hurtigt som muligt inden for rammerne af de relevante kontraktlige ordninger. Den finansielle enhed skal dokumentere den planlagte tidsplan for gennemførelsen.

2. Politikken skal fastlægge eller henvise til en metode til bestemmelse af, hvilke IKT-tjenester der understøtter kritiske eller vigtige funktioner. Politikken skal også angive, hvornår denne vurdering skal foretages og gennemgås.

3. Politikken skal indeholde en klar tildeling af det interne ansvar for godkendelse, forvaltning, kontrol og dokumentation af relevante kontraktlige ordninger og sikrer, at den finansielle enhed opretholder passende færdigheder, erfaring og viden med henblik på effektivt at føre tilsyn med de relevante kontraktlige ordninger, herunder de IKT-tjenester, der leveres i henhold til disse ordninger.

4. Uden at det berører den finansielle enheds endelige ansvar for effektivt at føre tilsyn med relevante kontraktlige ordninger, skal politikken indeholde krav om, at tredjepartsudbyderen af IKT-tjenester vurderes at have tilstrækkelige ressourcer til at sikre, at den finansielle enhed efterlever alle sine retlige og forskriftsmæssige krav vedrørende de IKT-tjenester, der understøtter de kritiske eller vigtige funktioner, der leveres.

5. Politikken skal klart angive den rolle eller det medlem af den øverste ledelse, der har ansvar for at overvåge de relevante kontraktlige ordninger. Politikken skal præcisere, hvordan denne rolle eller dette medlem af den øverste ledelse skal samarbejde med kontrolfunktionerne, medmindre denne er del af dem, og fastlægge rapporteringsvejene til ledelsesorganet, herunder arten af de oplysninger, der skal indberettes, og de dokumenter, der skal fremlægges. Den skal også fastsætte hyppigheden af sådanne indberetninger.

6. Politikken skal sikre, at de kontraktlige ordninger er i overensstemmelse med følgende:

a) den ramme for IKT-risikostyring, der er omhandlet i artikel 6, i forordning (EU) 2022/2554

b) den informationssikkerhedspolitik, der er omhandlet i artikel 9, stk. 4, i forordning (EU) 2022/2554

c) den politik for IKT-driftsstabilitet, der er omhandlet i artikel 11 i forordning (EU) 2022/2554

d) de krav vedrørende indberetningen af hændelser, der er omhandlet i artikel 19 i forordning (EU) 2022/2554.

7. Politikken skal indeholde krav om, at IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester, underkastes en uafhængig gennemgang og indgår i revisionsplanen.

8. Det skal udtrykkeligt fremgå af politikken, at de kontraktlige ordninger:

a) ikke fritager den finansielle enhed og dens ledelsesorgan for dens forpligtelser og ansvar over for kunderne

b) ikke må forhindre et effektivt tilsyn med en finansiel enhed og ikke må være i strid med eventuelle tilsynsmæssige begrænsninger for tjenester og aktiviteter

c) skal indeholde krav om, at tredjepartsudbydere af IKT-tjenester samarbejder med de kompetente myndigheder

d) skal indeholde krav om, at den finansielle enhed, dens revisorer og kompetente myndigheder har effektiv adgang til data og lokaler, som har relation til brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 4

Hovedfaserne i livscyklussen for vedtagelse og brug af kontraktlige ordninger

Politikken skal beskrive kravene, herunder reglerne, ansvarsområderne og processerne, for hver af hovedfaserne i den kontraktlige ordnings livscyklus, der som minimum omfatter følgende:

a) ledelsesorganets ansvarsområder, herunder, hvis det er relevant, inddragelse i beslutningsprocessen vedrørende brugen af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af IKT-tjenester

b) planlægningen af kontraktlige ordninger, herunder risikovurderingen, due diligence, jf. artikel 5 og 6, og godkendelsesprocessen for nye eller væsentlige ændringer af disse kontraktlige ordninger, jf. artikel 8, stk. 4

c) inddragelse af forretningsenheder, interne kontroller og andre relevante enheder i forbindelse med kontraktlige ordninger

d) gennemførelse, overvågning og forvaltning af kontraktlige ordninger, jf. artikel 7, 8 og 9, herunder på konsolideret og delkonsolideret grundlag, hvis det er relevant

e) dokumentation og registrering, idet der tages hensyn til kravene vedrørende det register over oplysninger, der er fastsat i artikel 28, stk. 3, i forordning (EU) 2022/2554

f) exitstrategierne og opsigelsesprocesserne, jf. artikel 10.

Artikel 5

Forudgående risikovurdering

1. Politikken skal indeholde krav om, at den finansielle enheds forretningsmæssige behov defineres, inden der indgås en kontraktlig ordning.

2. Politikken skal indeholde krav om, at der foretages en risikovurdering på finansenhedsniveau og, hvis det er relevant, på konsolideret og delkonsolideret grundlag, inden der indgås en kontraktlig ordning.

Risikovurderingen skal tage hensyn til alle de relevante krav, der er fastsat i forordning (EU) 2022/2554 og gældende sektorspecifik EU-lovgivning. Den skal navnlig tage hensyn til indvirkningen af leveringen fra tredjepartsudbydere af IKT-tjenester af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, på den finansielle enhed og alle de risici, der er forbundet med leveringen fra tredjepartsudbydere af IKT-tjenester af disse IKT-tjenester, der understøtter kritiske eller vigtige funktioner, herunder følgende:

a) operationelle risici

b) retlige risici

c) IKT-risici

d) omdømmemæssige risici

e) risici forbundet med beskyttelse af fortrolige oplysninger eller personoplysninger

f) risici forbundet med tilgængeligheden af data

g) risici forbundet med det sted, hvor dataene behandles og lagres

h) risici forbundet med det sted, hvor tredjepartsudbyderen af IKT-tjenester er beliggende

i) IKT-koncentrationsrisici på enhedsniveau.

Artikel 6

Due diligence

1. Politikken skal fastsætte en passende og forholdsmæssigt afstemt proces for udvælgelse og vurdering af potentielle tredjepartsudbydere af IKT-tjenester, idet der tages hensyn til, om tredjepartsudbyderen af IKT-tjenester er en koncernintern udbyder af IKT-tjenester, og skal indeholde krav om, at den finansielle enhed, inden den indgår en kontraktlig ordning, vurderer, om tredjepartsudbyderen af IKT-tjenester:

a) har det virksomhedsomdømme, de tilstrækkelige evner, den ekspertise og de tilstrækkelige finansielle, menneskelige og tekniske ressourcer, de informationssikkerhedsstandarder, den passende organisatoriske struktur, den risikostyring og de interne kontroller og, hvis det er relevant, de nødvendige tilladelser eller registreringer, der skal til for at levere de IKT-tjenester, der understøtter den kritiske eller vigtige funktion, på en pålidelig og professionel måde

b) er i stand til at overvåge den relevante teknologiske udvikling og identificere førende praksis inden for IKT-sikkerhed og gennemføre den, hvis det er relevant, for at have en effektiv og solid ramme for digital operationel modstandsdygtighed

c) anvender eller har til hensigt at anvende IKT-underleverandører til at udføre IKT-tjenester, der understøtter kritiske eller vigtige funktioner eller væsentlige dele heraf

d) er beliggende i eller behandler eller lagrer dataene i et tredjeland, og, hvis dette er tilfældet, om denne praksis påvirker omfanget af operationelle eller omdømmemæssige risici eller risikoen for at blive berørt af restriktive foranstaltninger, herunder embargoer og sanktioner, som kan påvirke tredjepartsudbyderens evne til at levere IKT-tjenesterne eller den finansielle enheds mulighed for at modtage disse IKT-tjenester

e) giver sit samtykke til kontraktlige ordninger, der sikrer, at selve den finansielle enhed, udpegede tredjeparter og kompetente myndigheder rent faktisk har mulighed for at foretage revisioner hos tredjepartsudbyderen af IKT-tjenester, herunder på stedet

f) handler på en etisk og socialt ansvarlig måde, respekterer menneskerettighederne og børns rettigheder, herunder forbuddet mod børnearbejde, overholder gældende principper om miljøbeskyttelse og sikrer passende arbejdsvilkår.

2. Politikken skal indeholde en beskrivelse af den krævede grad af garanti med hensyn til effektiviteten af risikostyringsrammen for tredjepartsudbydere af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, og som skal leveres af en tredjepartsudbyder af IKT-tjenester. Politikken skal indeholde krav om, at due diligence-processen omfatter en vurdering af, hvorvidt der findes risikobegrænsende foranstaltninger og foranstaltninger til driftsstabilitet, og af, hvordan det sikres, at de fungerer hos tredjepartsudbyderen af IKT-tjenester.

3. Politikken skal fastlægge due diligence-processen for udvælgelse og vurdering af potentielle tredjepartsudbydere af IKT-tjenester og angive, hvilke af følgende elementer der skal anvendes på det påkrævede tillidsniveau for tredjepartsudbyderens resultater:

a) revisioner eller uafhængige vurderinger foretaget af den finansielle enhed selv eller på dennes vegne

b) anvendelse af uafhængige revisionsrapporter udarbejdet efter anmodning fra tredjepartsudbyderen af IKT-tjenester

c) anvendelse af revisionsrapporter udarbejdet af den interne revisionsfunktion hos tredjepartsudbyderen af IKT-tjenester

d) anvendelse af passende tredjepartscertificeringer

e) anvendelse af andre relevante oplysninger, der er tilgængelige for den finansielle enhed, eller andre oplysninger fra tredjepartsudbyderen af IKT-tjenester.

4. Finansielle enheder sikrer en passende grad af garanti for det præstationsniveau, der leveres af tredjepartsudbyderen af IKT-tjenester, idet der tages hensyn til de elementer, der er angivet i stk. 3, litra a)-e). Hvis det er relevant, skal der anvendes mere end ét af de elementer, der er angivet under disse punkter.

Artikel 7

Interessekonflikter

1. Politikken skal indeholde en beskrivelse af passende foranstaltninger til at identificere, forebygge og håndtere faktiske eller potentielle interessekonflikter, der opstår som følge af brugen af tredjepartsudbydere af IKT-tjenester, og som skal træffes, inden der indgås relevante kontraktlige ordninger, og skal indeholde bestemmelser om løbende overvågning af sådanne interessekonflikter.

2. Hvis IKT-tjenester, der understøtter kritiske eller vigtige funktioner, leveres af koncerninterne udbydere af IKT-tjenester, skal det i politikken præciseres, at beslutninger om betingelserne, herunder de finansielle betingelser, for IKT-tjenesterne skal træffes objektivt.

Artikel 8

Kontraktbestemmelser

1. Politikken skal præcisere, at den relevante kontraktlige ordning skal foreligge i skriftlig form og omfatte alle de elementer, der er omhandlet i artikel 30, stk. 2 og 3, i forordning (EU) 2022/2554. Politikken skal også omfatte elementer vedrørende de krav, der er omhandlet i artikel 1, stk. 1, litra a), i forordning (EU) 2022/2554, samt anden relevant EU-ret og national ret, alt efter hvad der er relevant.

2. Politikken skal præcisere, at de relevante kontraktlige ordninger skal omfatte den finansielle enheds ret til at opnå adgang til oplysninger, til at udføre inspektioner og revisioner og til at udføre test af IKT. Med henblik herpå skal politikken indeholde krav om, at den finansielle enhed anvender følgende metoder, uden at dette berører den finansielle enheds endelige ansvar:

a) dens egen interne revision eller en revision foretaget af en udpeget tredjepart

b) hvis det er relevant, fælles revisioner og fælles IKT-test, herunder trusselsbaseret penetrationstest, der tilrettelægges i fællesskab med andre ordregivende finansielle enheder eller virksomheder, der anvender IKT-tjenester fra den samme tredjepartsudbyder af IKT-tjenester, og som foretages af disse ordregivende finansielle enheder eller virksomheder eller af en tredjepart, som de har udpeget

c) hvis det er relevant, tredjepartscertificeringer

d) hvis det er relevant, interne revisionsrapporter eller revisionsrapporter fra tredjeparter, som tredjepartsudbyderen af IKT-tjenester stiller til rådighed.

3. Den finansielle enhed må ikke over tid udelukkende forlade sig på certificeringer som omhandlet i stk. 2, litra c), eller revisionsrapporter som omhandlet i nævnte stykkes litra d). Politikken må kun tillade anvendelse af de metoder, der er omhandlet i stk. 2, litra c) og d), såfremt den finansielle enhed:

a) finder revisionsplanen fra tredjepartsudbyderen af IKT-tjenester tilfredsstillende i forhold til de relevante kontraktlige ordninger

b) sørger for, at certificerings-eller revisionsrapporternes anvendelsesområde inddrager de systemer og centrale kontroller, som de har identificeret, og sikrer efterlevelse af relevante forskriftsmæssige krav

c) foretager en løbende grundig vurdering af certificerings- eller revisionsrapporternes indhold og efterprøver, at rapporterne eller certificeringerne ikke er forældede

d) sikrer, at de centrale systemer og kontroller inddrages i fremtidige versioner af certificerings- eller revisionsrapporten

e) finder certificerings- eller revisionsvirksomheden tilfredsstillende egnet

f) finder det godtgjort, at certificeringerne udstedes, og at revisionerne udføres på grundlag af bredt anerkendte relevante faglige standarder og omfatter en test af den operationelle effektivitet af de centrale kontroller, der er indført

g) har kontraktlig ret til med en hyppighed, der er rimelig og legitim ud fra et risikostyringsperspektiv, at anmode om ændringer af anvendelsesområdet for certificerings- eller revisionsrapporter med henblik på at inddrage andre relevante systemer og kontroller

h) har kontraktlig ret til at udføre individuelle og fælles revisioner efter eget skøn med hensyn til de kontraktlige ordninger og udøve disse rettigheder i henhold til den aftalte hyppighed.

4. Politikken skal sikre, at væsentlige ændringer af den kontraktlige ordning formaliseres i et skriftligt dokument, der er dateret og underskrevet af alle parter, og som skal angive processen for fornyet indgåelse af de kontraktlige ordninger.

Artikel 9

Overvågning af de kontraktlige ordninger

1. Politikken skal indeholde krav om, at de kontraktlige ordninger beskriver foranstaltninger og centrale indikatorer til løbende overvågning af det præstationsniveau, der leveres af tredjepartsudbydere af IKT-tjenester, herunder foranstaltninger til overvågning af overholdelsen af kravene vedrørende fortroligheden, tilgængeligheden, integriteten og autenticiteten af data og oplysninger og af, om tredjepartsudbyderen af IKT-tjenester efterlever den finansielle enheds relevante politikker og procedurer. Politikken skal også præcisere de foranstaltninger, der finder anvendelse, når serviceniveauaftaler ikke overholdes, herunder kontraktlige sanktioner, hvis det er relevant.

2. Politikken skal præcisere, hvordan den finansielle enhed skal vurdere, hvorvidt de tredjepartsudbydere af IKT-tjenester, der anvendes til de IKT-tjenester, der understøtter kritiske eller vigtige funktioner, opfylder passende standarder for præstationsniveau og kvalitet i overensstemmelse med den kontraktlige ordning og den finansielle enheds egne politikker. Politikken skal navnlig sikre følgende:

a) at tredjepartsudbyderne af IKT-tjenester forelægger passende rapporter om deres aktiviteter og tjenester til den finansielle enhed, herunder periodiske rapporter, hændelsesrapporter, rapporter om levering af tjenester, rapporter om IKT-sikkerhed og rapporter om foranstaltninger til sikring af driftsstabilitet og test

b) at det præstationsniveau, der leveres af tredjepartsudbyderen af IKT-tjenester, vurderes ved hjælp af centrale resultatindikatorer, centrale kontrolindikatorer, revisioner, selvcertificeringer og uafhængige gennemgange i overensstemmelse med den finansielle enheds ramme for IKT-risikostyring

c) at den finansielle enhed modtager andre relevante oplysninger fra tredjepartsudbyderne af IKT-tjenester

d) at den finansielle enhed, hvis det er relevant, underrettes om IKT-relaterede hændelser og operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser

e) at der foretages en uafhængig gennemgang og uafhængige revisioner, der efterprøver overholdelsen af lov- og forskriftsmæssige krav og politikker.

3. Politikken skal præcisere, at den i stk. 2 omhandlede vurdering skal dokumenteres, og at resultaterne heraf skal anvendes til at ajourføre den finansielle enheds risikovurdering, jf. artikel 6.

4. Politikken skal fastlægge passende foranstaltninger, som den finansielle enhed skal træffe, hvis den konstaterer mangler hos tredjepartsudbydere af IKT-tjenester, herunder IKT-relaterede hændelser og operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, i forbindelse med leveringen af de IKT-tjenester, der understøtter kritiske eller vigtige funktioner, eller i overensstemmelse med kontraktlige ordninger eller retlige krav. Den skal også præcisere, hvordan gennemførelsen af sådanne foranstaltninger skal overvåges for at sikre, at de rent faktisk overholdes inden for en fastsat tidsramme, idet der tages hensyn til manglernes væsentlighed.

Artikel 10

Udtræden og opsigelse af kontraktlige ordninger:

Politikken skal indeholde krav om en dokumenteret exitplan for hver kontraktlig ordning og om periodisk gennemgang og test af den dokumenterede exitplan. Ved udarbejdelsen af exitplanen skal der tages hensyn til følgende:

a) uforudsete og vedvarende driftsafbrydelser

b) uhensigtsmæssig eller mislykket levering af tjenester

c) uventet opsigelse af den kontraktlige ordning.

Exitplanen skal være realistisk, gennemførlig, baseret på plausible scenarier og rimelige antagelser og skal indeholde en planlagt gennemførelsesplan, der er forenelig med de udtrædelses- og opsigelsesvilkår, der er fastsat i de kontraktlige ordninger.

Artikel 11

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 13. marts 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand