Publicatieblad
van de Europese Unie

NL
L-serie

2024/1773

25.6.2024

GEDELEGEERDE VERORDENING (EU) 2024/1773 VAN DE COMMISSIE

van 13 maart 2024

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad betreffende technische reguleringsnormen tot bepaling van de gedetailleerde inhoud van het beleid met betrekking tot de contractuele overeenkomsten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 28, lid 10, derde alinea,

Overwegende hetgeen volgt:

(1) Het bij Verordening (EU) 2022/2554 vastgestelde kader voor digitale operationele weerbaarheid voor de financiële sector vereist dat financiële entiteiten bepaalde kernbeginselen vaststellen voor het beheer van ICT-risico's van derden, die des te belangrijker zijn wanneer financiële entiteiten er ondersteuning van kritieke of belangrijke functies een beroep op derde aanbieders van ICT-diensten doen.

(2) Financiële entiteiten moeten, als onderdeel van hun kader voor ICT-risicobeheer, een strategie inzake ICT-risico van derde aanbieders vaststellen en deze regelmatig herzien. Overeenkomstig artikel 28, lid 2, van Verordening (EU) 2022/2554 moet die strategie een beleid omvatten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen. Zij moet van toepassing zijn op individuele basis en, in voorkomend geval, op gesubconsolideerde en geconsolideerde basis.

(3) Financiële entiteiten lopen sterk uiteen in omvang, structuur en interne organisatie en in de aard en complexiteit van hun activiteiten en activiteiten. Bij de ontwikkeling van het beleid met betrekking tot de contractuele overeenkomsten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen ("het beleid") moet rekening worden gehouden met deze diversiteit maar moeten ook bepaalde fundamentele regelgevingsvereisten worden opgelegd die passend zijn voor alle financiële entiteiten, en moet ervoor worden gezorgd dat die vereisten op evenredige wijze worden toegepast.

(4) Wanneer financiële entiteiten tot een groep behoren, moet de moederonderneming die verantwoordelijk is voor het verstrekken van de geconsolideerde of gesubconsolideerde financiële overzichten voor de groep er daarom voor zorgen dat het beleid binnen de groep op consistente en coherente wijze wordt toegepast.

(5) Bij de toepassing van het beleid moeten aanbieders van ICT-diensten binnen een groep, met inbegrip van aanbieders van ICT-diensten die geheel of gedeeltelijk eigendom zijn van financiële entiteiten binnen hetzelfde institutionele protectiestelsel, worden beschouwd als derde aanbieders van ICT-diensten. De risico's van aanbieders van ICT-diensten binnen een groep kunnen verschillen, maar de vereisten die op hen van toepassing zijn, zijn dezelfde uit hoofde van Verordening (EU) 2022/2554. Op soortgelijke wijze moet het beleid van toepassing zijn op subcontractanten die ICT-diensten verlenen ter ondersteuning van kritieke of belangrijke functies of materiële delen daarvan aan derde aanbieders van ICT-diensten, wanneer er een keten van derde aanbieders van ICT-diensten bestaat.

(6) De uiteindelijke verantwoordelijkheid van het leidinggevend orgaan voor het beheer van het ICT-risico van een financiële entiteit is een overkoepelend beginsel dat ook van toepassing is op het gebruik van derde aanbieders van ICT-diensten. Deze verantwoordelijkheid moet verder worden vertaald een voortdurende betrokkenheid van het leidinggevend orgaan bij de controle van de monitoring van het ICT-risicobeheer, met inbegrip van de vaststelling en evaluatie, ten minste eenmaal per jaar, van het beleid.

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

(7) Om een passende rapportage aan het leidinggevend orgaan te waarborgen, moeten in het beleid de interne verantwoordelijkheden voor de goedkeuring, het beheer, de controle en de documentatie van contractuele overeenkomsten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen ("contractuele overeenkomsten"), met inbegrip van de ICT-diensten die worden verleend in het kader van contractuele overeenkomsten als bedoeld in artikel 28, lid 1, punt a), van Verordening (EU) 2022/2554, duidelijk worden gespecificeerd en geïdentificeerd.

(8) Om rekening te houden met alle mogelijke risico's die zich kunnen voordoen bij het sluiten van contracten voor ICT-diensten die kritieke of belangrijke functies ondersteunen, moet de structuur van het beleid alle stappen van elke hoofdfase van de levenscyclus volgen voor contractuele overeenkomsten met derde aanbieders.

(9) Om de geconstateerde risico's te mitigeren, moet het beleid de planning van contractuele overeenkomsten specificeren, met inbegrip van de risicobeoordeling, de zorgvuldigheid en het goedkeuringsproces voor nieuwe of materiële wijzigingen in die contractuele regelingen. Om de risico's te beheren die zich kunnen voordoen voordat een contractuele overeenkomst met een derde aanbieder van ICT-diensten wordt gesloten, moet in het beleid een passend en evenredig proces worden gespecificeerd om potentiële derde aanbieders van ICT-diensten te selecteren en hun geschiktheid te beoordelen, en moet de financiële entiteit rekening houden met een niet-uitputtende lijst van elementen waarover de derde aanbieders van ICT-diensten moeten beschikken. De lijst moet elementen bevatten die verband houden met de zakelijke reputatie van de dienstverleners, hun financiële, personele en technische middelen, hun informatiebeveiliging, hun organisatiestructuur, met inbegrip van risicobeheer, en hun interne controles.

(10) Om te zorgen voor een degelijk risicobeheer bij het verlenen van ICT-diensten ter ondersteuning van kritieke of belangrijke functies door derde aanbieders van ICT-diensten, moet het beleid informatie bevatten over de uitvoering en het beheer van en het toezicht op de contractuele overeenkomsten, in voorkomend geval ook op geconsolideerd en gesubconsolideerd niveau. Dit omvat vereisten voor de contractuele bepalingen inzake wederzijdse verplichtingen van de financiële entiteiten en de derde aanbieders van ICT-diensten, die schriftelijk moeten worden vastgelegd. Om efficiënt toezicht te waarborgen en weerbaarheid te bevorderen in geval van veranderingen in het bedrijfsmodel of het ondernemingsklimaat, moet het beleid het recht van financiële entiteiten of aangestelde derden en bevoegde autoriteiten op inspecties en toegang tot informatie waarborgen, en moet het ook de exitstrategieën en beëindigingsprocessen nader specificeren.

(11) Voor zover persoonsgegevens door derde aanbieders van ICT-diensten worden verwerkt, doen dit beleid en eventuele contractuele overeenkomsten geen afbreuk aan en moeten zij een aanvulling vormen op de verplichtingen uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([2]), zoals het beschikken over een schriftelijk contract waarin de verwerking van persoonsgegevens wordt beschreven, de verplichting om de beveiliging van de verwerking van persoonsgegevens te waarborgen en het vaststellen van alle andere elementen die uit hoofde van die verordening vereist zijn.

([2]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Het Gemengd Comité van de Europese toezichthoudende autoriteiten als bedoeld in artikel 54 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([3]), in artikel 54 van Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([4]) en in artikel 54 van Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad ([5]) heeft open publiek consultaties gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, heeft de mogelijke kosten en baten van die voorgestelde normen geanalyseerd en heeft het advies ingewonnen van de overeenkomstig artikel 37 van Verordening (EU) nr. 1093/2010 opgerichte Stakeholdergroep bankwezen, de overeenkomstig artikel 37 van Verordening (EU) nr. 1094/2010 opgerichte Stakeholdergroep verzekeringen en herverzekeringen en de overeenkomstig artikel 37 van Verordening (EU) nr. 1095/2010 opgerichte Stakeholdergroep effecten en markten.

(13) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) en heeft op 24 januari 2024 een advies uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Algeheel risicoprofiel en complexiteit

In het beleid inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen ("het beleid") wordt rekening gehouden met de omvang en het algehele risicoprofiel van de financiële entiteit en met de aard, schaal en elementen van de toegenomen of verminderde complexiteit van haar diensten, activiteiten en verrichtingen, met inbegrip van elementen die verband houden met:

(a) het soort ICT-diensten dat is opgenomen in de contractuele overeenkomst inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen ("de contractuele overeenkomst") tussen de financiële entiteit en de derde aanbieder van ICT-diensten;

(b) de locatie van de derde aanbieder van ICT-diensten of de locatie van zijn moederonderneming;

(c) of de ICT-diensten die kritieke of belangrijke functies ondersteunen, worden verleend door een derde aanbieder van ICT-diensten die zich in een lidstaat of in een derde land bevindt, ook rekening houdend met de locatie van waaruit de ICT-diensten worden verleend en de locatie waar de gegevens worden verwerkt en opgeslagen;

(d) de aard van de gegevens die met de derde aanbieder van ICT-diensten worden gedeeld;

(e) of de derde aanbieder van ICT-diensten deel uitmaakt van dezelfde groep als de financiële entiteit waaraan de diensten worden verleend;

([3]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84), ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(f) het gebruik van derde aanbieders van ICT-diensten die een vergunning hebben gekregen van, geregistreerd zijn of aan toezicht of oversight onderworpen zijn door een bevoegde autoriteit in een lidstaat, of onderworpen zijn aan het oversightkader uit hoofde van hoofdstuk V, afdeling II, van Verordening (EU) 2022/2554, en het gebruik van andere derde aanbieders van ICT-diensten;

(g) het gebruik van derde aanbieders van ICT-diensten die een vergunning hebben gekregen van, geregistreerd zijn of aan toezicht of oversight onderworpen zijn door een toezichthoudende autoriteit in een derde land, en het gebruik van andere derde aanbieders van ICT-diensten;

(h) of de verlening van ICT-diensten ter ondersteuning van kritieke of belangrijke functies geconcentreerd is op één derde aanbieder van ICT-diensten of op een klein aantal dergelijke dienstverleners;

(i) de overdraagbaarheid van de ICT-diensten die kritieke of belangrijke functies ondersteunen naar een andere derde aanbieder van ICT-diensten, ook als gevolg van specifieke technologische kenmerken;

(j) de mogelijke gevolgen van verstoringen in de verlening van ICT-diensten ter ondersteuning van kritieke of belangrijke functies voor de continuïteit van de activiteiten van de financiële entiteit en voor de beschikbaarheid van haar diensten.

Artikel 2

Toepassing in de groep

Indien deze verordening op gesubconsolideerde of geconsolideerde basis van toepassing is, zorgt de moederonderneming die verantwoordelijk is voor het verstrekken van de geconsolideerde of gesubconsolideerde financiële overzichten voor de groep ervoor dat het beleid consequent wordt toegepast in alle financiële entiteiten die deel uitmaken van de groep en toereikend is voor de effectieve toepassing van deze verordening op alle relevante niveaus van de groep.

Artikel 3

Governanceregelingen

1. Het leidinggevend orgaan evalueert het beleid ten minste eenmaal per jaar en werkt het zo nodig bij. Wijzigingen in het beleid worden tijdig uitgevoerd en zo spoedig als mogelijk is binnen de relevante contractuele overeenkomsten. De financiële entiteit documenteert het geplande tijdschema voor de uitvoering.

2. Het beleid voorziet in of verwijst naar een methode om te bepalen welke ICT-diensten kritieke of belangrijke functies ondersteunen. In het beleid wordt ook gespecificeerd wanneer deze beoordeling moet worden uitgevoerd en geëvalueerd.

3. In het beleid worden de interne verantwoordelijkheden voor de goedkeuring, het beheer, de controle en de documentatie van relevante contractuele overeenkomsten duidelijk toegewezen en wordt gewaarborgd dat binnen de financiële entiteit passende vaardigheden, ervaring en kennis in stand worden gehouden om effectief toezicht te houden op de relevante contractuele overeenkomsten, met inbegrip van de ICT-diensten die in het kader van die overeenkomsten worden verleend.

4. Onverminderd de eindverantwoordelijkheid van de financiële entiteit om effectief toezicht te houden op relevante contractuele regelingen, moet het beleid vereisen dat de derde aanbieder van ICT-diensten wordt geacht over voldoende middelen te beschikken om ervoor te zorgen dat de financiële entiteit voldoet aan al haar wettelijke en regelgevingsvereisten met betrekking tot de ICT-diensten die kritieke of belangrijke functies ondersteunen.

5. In het beleid wordt duidelijk aangegeven welke rol of welk lid van het hoger leidinggevend personeel verantwoordelijk is voor het toezicht op de relevante contractuele overeenkomsten. In het beleid wordt gespecificeerd hoe die rol of dat lid van het hoger leidinggevend personeel met de controlefuncties samenwerkt, tenzij die/dat er deel van uitmaakt, en worden de rapportagelijnen voor het leidinggevend orgaan vastgesteld, met inbegrip van de aard van de te rapporteren informatie en de te verstrekken documenten. In het verslag wordt ook de frequentie van die rapportage vastgesteld.

6. Het beleid waarborgt dat de contractuele overeenkomsten in overeenstemming zijn met het volgende:

(a) het in artikel 6 van Verordening (EU) 2022/2554 bedoelde kader voor ICT-risicobeheer;

(b) het in artikel 9, lid 4, van Verordening (EU) 2022/2554 bedoelde beleid inzake informatiebeveiliging;

(c) het in artikel 11 van Verordening (EU) 2022/2554 bedoelde beleid inzake ICT-bedrijfscontinuïteit;

(d) de in artikel 19 van Verordening (EU) 2022/2554 bedoelde vereisten voor de rapportage van incidenten.

7. Het beleid vereist dat ICT-diensten ter ondersteuning van kritieke of belangrijke functies die door derde aanbieders van ICT-diensten worden verleend, aan een onafhankelijke evaluatie worden onderworpen en in het auditplan worden opgenomen.

8. In het beleid wordt uitdrukkelijk gespecificeerd dat de contractuele overeenkomsten:

(a) de financiële entiteit en haar leidinggevend orgaan niet ontslaan van hun wettelijke verplichtingen en verantwoordelijkheden jegens hun cliënten;

(b) doeltreffend toezicht op een financiële entiteit niet mogen belemmeren en niet in strijd mogen zijn met eventuele beperkingen van het toezicht op diensten en activiteiten;

(c) moeten vereisen dat derde aanbieders van ICT-diensten samenwerken met de bevoegde autoriteiten;

(d) moeten vereisen dat de financiële entiteit, haar auditors en de bevoegde autoriteiten effectieve toegang hebben tot gegevens en gebouwen met betrekking tot het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen.

Artikel 4

Belangrijkste fasen van de levenscyclus voor de vaststelling en het gebruik van contractuele overeenkomsten

Het beleid specificeert de eisen, met inbegrip van de regels, de verantwoordelijkheden en de processen, voor elke hoofdfase van de levenscyclus van de contractuele overeenkomst, met betrekking tot ten minste het volgende:

(a) de verantwoordelijkheden van het leidinggevend orgaan, met inbegrip van zijn betrokkenheid, in voorkomend geval, bij het besluitvormingsproces over het gebruik van ICT-diensten ter ondersteuning van kritieke of belangrijke functies die door derde aanbieders van ICT-diensten worden verleend;

(b) de planning van contractuele overeenkomsten, met inbegrip van de risicobeoordeling, de zorgvuldigheid als bedoeld in de artikelen 5 en 6 en het goedkeuringsproces met betrekking tot nieuwe of materiële wijzigingen in contractuele overeenkomsten als bedoeld in artikel 8, lid 4;

(c) de betrokkenheid van bedrijfseenheden, interne controles en andere relevante eenheden met betrekking tot contractuele regelingen;

(d) de uitvoering, de monitoring en het beheer van contractuele overeenkomsten als bedoeld in de artikelen 7, 8 en 9, ook op geconsolideerd en gesubconsolideerd niveau, indien van toepassing;

(e) de documentatie en het bijhouden van registers, rekening houdend met de voorschriften inzake het informatieregister als bedoeld in artikel 28, lid 3, van Verordening (EU) 2022/2554;

(f) de exitstrategieën en beëindigingsprocessen als bedoeld in artikel 10.

Artikel 5

Risicobeoordeling vooraf

1. Het beleid vereist dat de bedrijfsbehoeften van de financiële entiteit worden vastgesteld voordat een contractuele overeenkomst wordt gesloten.

2. Het beleid vereist dat een risicobeoordeling wordt uitgevoerd op het niveau van de financiële entiteit en, in voorkomend geval, op geconsolideerd en gesubconsolideerd niveau voordat een contractuele overeenkomst wordt gesloten.

Bij de risicobeoordeling wordt rekening gehouden met alle relevante voorschriften van Verordening (EU) 2022/2554 en de toepasselijke sectorale wetgeving van de Unie. Er wordt met name rekening gehouden met de gevolgen van het verlenen van ICT-diensten ter ondersteuning van kritieke of belangrijke functies door derde aanbieders van ICT-diensten voor de financiële entiteit en alle risico's die verbonden zijn aan het verlenen van ICT-diensten ter ondersteuning van kritieke of belangrijke functies door derde aanbieders van ICT-diensten, met inbegrip van:

(a) operationele risico's;

(b) juridische risico's;

(c) ICT-risico's;

(d) reputatierisico's:

(e) risico's in verband met de bescherming van vertrouwelijke of persoonsgegevens;

(f) risico's in verband met de beschikbaarheid van gegevens;

(g) risico's in verband met de plaats waar de gegevens worden verwerkt en opgeslagen;

(h) risico's in verband met de locatie van de derde aanbieder van ICT-diensten;

(i) ICT-concentratierisico op het niveau van de entiteit.

Artikel 6

Zorgvuldigheid

1. Het beleid voorziet in een passend en evenredig proces voor de selectie en beoordeling van de potentiële derde aanbieders van ICT-diensten, rekening houdend met de vraag of de derde aanbieder van ICT-diensten al dan niet een aanbieder van ICT-diensten binnen de groep is, en vereist dat de financiële entiteit, alvorens een contractuele overeenkomst aan te gaan, beoordeelt of de derde aanbieder van ICT-diensten:

(a) een goede zakelijke reputatie heeft en beschikt over voldoende capaciteiten, deskundigheid en adequate financiële, personele en technische middelen, normen voor informatiebeveiliging, passende organisatiestructuur, risicobeheer en interne controles en, indien van toepassing, over de vereiste vergunningen of registraties om de ICT-diensten ter ondersteuning van de kritieke of belangrijke functie op betrouwbare en professionele wijze te verlenen;

(b) in staat is relevante technologische ontwikkelingen te monitoren en leidende praktijken op het gebied van ICT-beveiliging in kaart te brengen en in voorkomend geval toe te passen met het oog op een doeltreffend en degelijk kader voor digitale operationele weerbaarheid;

(c) ICT-subcontractanten gebruikt of voornemens is deze te gebruiken voor de uitvoering van de ICT-diensten die kritieke of belangrijke functies ondersteunen, of materiële onderdelen daarvan;

(d) zich in een derde land bevindt of daar de gegevens verwerkt of opslaat en, indien dit het geval is, of deze praktijk van invloed is op het niveau van operationele of reputatierisico's of op het risico te worden getroffen door beperkende maatregelen, met inbegrip van embargo's en sancties, die van invloed kunnen zijn op het vermogen van de derde aanbieder van ICT-diensten om de ICT-diensten te verlenen of de financiële entiteit om die ICT-diensten te ontvangen;

(e) instemt met contractuele overeenkomsten die waarborgen dat het daadwerkelijk mogelijk is audits uit te voeren bij de derde aanbieder van ICT-diensten, ook ter plaatse, door de financiële entiteit zelf, aangestelde derde partijen en bevoegde autoriteiten;

(f) op ethische en maatschappelijk verantwoorde wijze handelt, de mensenrechten en de rechten van het kind, met inbegrip van het verbod op kinderarbeid, eerbiedigt, de toepasselijke beginselen inzake milieubescherming eerbiedigt en voor passende arbeidsomstandigheden zorgt.

2. Het beleid specificeert het vereiste zekerheidsniveau met betrekking tot de doeltreffendheid van het kader voor risicobeheer van derde aanbieders van ICT-diensten die cruciale of belangrijke functies ondersteunen die door een derde aanbieder van ICT-diensten moeten worden verricht. Het beleid vereist dat het zorgvuldigheidsproces een beoordeling omvat van het bestaan van risicobeperkende en bedrijfscontinuïteitsmaatregelen en van de wijze waarop de werking ervan binnen de derde aanbieder van ICT-diensten wordt gewaarborgd.

3. In het beleid wordt het zorgvuldigheidsproces voor de selectie en beoordeling van de potentiële derde aanbieders van ICT-diensten vastgesteld en wordt aangegeven welke van de volgende elementen moeten worden gebruikt voor het vereiste zekerheidsniveau met betrekking tot de prestaties van de derde aanbieder van ICT-diensten:

(a) audits of onafhankelijke beoordelingen die door of namens de financiële entiteit worden uitgevoerd;

(b) het gebruik van onafhankelijke auditverslagen die op verzoek van de derde aanbieder van ICT-diensten worden opgesteld;

(c) het gebruik van auditverslagen van de interneauditfunctie van de derde aanbieder van ICT-diensten;

(d) het gebruik van passende certificeringen door derde partijen;

(e) het gebruik van andere relevante informatie waarover de financiële entiteit beschikt of andere door de derde aanbieder van ICT-diensten verstrekte informatie.

4. Financiële entiteiten zorgen voor een passend niveau van zekerheid over de prestaties van de derde aanbieder van ICT-diensten, rekening houdend met de in lid 3, punten a) tot en met e), genoemde elementen. Indien nodig worden meerdere in die punten genoemde elementen gebruikt.

Artikel 7

Belangenconflicten

1. Het beleid specificeert de passende maatregelen voor het identificeren, voorkomen en beheren van uit het gebruik van derde aanbieders van ICT-diensten voortvloeiende feitelijke of mogelijke belangenconflicten, die moeten worden genomen voordat relevante contractuele overeenkomsten worden gesloten, en voorziet in een permanente monitoring van dergelijke belangenconflicten.

2. Wanneer ICT-diensten ter ondersteuning van kritieke of belangrijke functies worden verleend door aanbieders van ICT-diensten binnen een groep, wordt in het beleid gespecificeerd dat besluiten over de voorwaarden, met inbegrip van de financiële voorwaarden, voor de ICT-diensten objectief moeten worden genomen.

Artikel 8

Contractuele bepalingen

1. Het beleid specificeert dat de relevante contractuele overeenkomsten schriftelijk moeten zijn opgesteld en alle in artikel 30, lid 2, en (3), van Verordening (EU) 2022/2554 bedoelde elementen moet bevatten. Het beleid omvat ook elementen met betrekking tot de in artikel 1, lid 1, punt a), van Verordening (EU) 2022/2554 bedoelde vereisten en, in voorkomend geval, andere relevante Unie- en nationale wetgeving.

2. Het beleid specificeert dat de relevante contractuele overeenkomsten het recht van de financiële entiteit moeten omvatten om toegang te krijgen tot informatie en om inspecties, audits en ICT-tests uit te voeren. Daartoe vereist het beleid dat de financiële entiteit de volgende methoden gebruikt, onverminderd de uiteindelijke verantwoordelijkheid van de financiële entiteit:

(a) haar eigen interne audit of een audit door een aangestelde derde partij;

(b) indien nodig, gebundelde audits en gebundelde ICT-tests, met inbegrip van dreigingsgestuurde penetratietests, die worden georganiseerd samen met andere aanbestedende financiële entiteiten of ondernemingen die gebruikmaken van ICT-diensten van dezelfde derde aanbieder van ICT-diensten en die worden uitgevoerd door die aanbestedende financiële entiteiten of bedrijven of door een door hen aangestelde derde partij;

(c) in voorkomend geval, certificeringen van derde partijen;

(d) in voorkomend geval, interne auditverslagen of auditverslagen van derde partijen die door de derde aanbieder van ICT-diensten ter beschikking worden gesteld.

3. De financiële entiteit mag zich in de loop der tijd niet uitsluitend blijven baseren op de in lid 2, punt c), bedoelde certificeringen of in punt d) van dat lid bedoelde auditverslagen. Het beleid staat het gebruik van de in lid 2, punten c) en d), bedoelde methoden alleen toe indien de financiële entiteit:

(a) tevreden is over het auditplan van de derde aanbieder van ICT-diensten voor de relevante contractuele overeenkomsten;

(b) ervoor zorgt dat het toepassingsgebied van de certificeringen of auditverslagen betrekking heeft op de door haar vastgestelde systemen en essentiële controles, en dat de naleving van de relevante regelgevingsvereisten wordt gewaarborgd;

(c) de inhoud van de certificeringen of auditverslagen doorlopend grondig beoordeelt en verifieert of de verslagen of certificeringen niet achterhaald zijn;

(d) ervoor zorgt dat essentiële systemen en controles in toekomstige versies van het certificerings- of auditverslag aan bod komen;

(e) tevreden is over de bekwaamheid van de certificerings- of auditpartij;

(f) ervan overtuigd is dat de certificeringen worden afgegeven en dat de audits worden uitgevoerd aan de hand van algemeen erkende relevante professionele normen en een test omvatten van de operationele doeltreffendheid van de bestaande essentiële controles;

(g) het contractuele recht heeft om, met een uit het oogpunt van risicobeheer redelijke en gerechtvaardigde frequentie, te verzoeken de certificeringen of auditverslagen uit te breiden naar andere relevante systemen en controles;

(h) het contractuele recht heeft om naar eigen goeddunken individuele en gebundelde audits met betrekking tot de contractuele overeenkomsten uit te voeren en die rechten uit te voeren in overeenstemming met de afgesproken frequentie.

4. Het beleid zorgt ervoor dat materiële wijzigingen in de contractuele overeenkomst worden geformaliseerd in een schriftelijk document dat door alle partijen is gedateerd en ondertekend, en vermeldt de verlengingsprocedure voor de contractuele overeenkomsten.

Artikel 9

Toezicht op de contractuele overeenkomsten

1. Het beleid vereist dat in de contractuele overeenkomsten de maatregelen en kernindicatoren worden gespecificeerd om de prestaties van derde aanbieders van ICT-diensten doorlopend te monitoren, met inbegrip van maatregelen om toe te zien op de naleving van de vereisten inzake vertrouwelijkheid, beschikbaarheid, integriteit en authenticiteit van gegevens en informatie en de naleving door de derde aanbieders van ICT-diensten van de relevante beleidslijnen en procedures van de financiële entiteit. In het beleid worden ook maatregelen gespecificeerd die van toepassing zijn wanneer de overeenkomsten inzake het dienstverleningsniveau niet worden nageleefd, met inbegrip van contractuele sancties indien nodig.

2. In het beleid wordt gespecificeerd hoe de financiële entiteit moet beoordelen of de derde aanbieders van ICT-diensten die kritieke of belangrijke functies ondersteunen, voldoen aan passende prestatie- en kwaliteitsnormen in overeenstemming met de contractuele overeenkomst en het eigen beleid van de financiële entiteit. Het beleid zorgt er met name voor:

(a) dat de derde aanbieders van ICT-diensten passende verslagen verstrekken over hun activiteiten en diensten aan de financiële entiteit, met inbegrip van periodieke verslagen, verslagen over incidenten, verslagen over de levering van diensten, verslagen over ICT-beveiliging en verslagen over bedrijfscontinuïteitsmaatregelen en -tests;

(b) dat de prestaties van derde aanbieders van ICT-diensten worden beoordeeld aan de hand van kernprestatie-indicatoren, kerncontrole-indicatoren, audits, zelfcertificeringen en onafhankelijke beoordelingen in overeenstemming met het kader voor ICT-risicobeheer van de financiële entiteit;

(c) dat de financiële entiteit andere relevante informatie van de derde aanbieders van ICT-diensten ontvangt;

(d) dat de financiële entiteit, in voorkomend geval, in kennis wordt gesteld van ICT-gerelateerde incidenten en betalingsgerelateerde operationele of beveiligingsincidenten;

(e) dat een onafhankelijke evaluatie en audits worden uitgevoerd om na te gaan of de vereisten en het beleid van wet- en regelgeving worden nageleefd.

3. In het beleid wordt gespecificeerd dat de in lid 2 bedoelde beoordeling moet worden gedocumenteerd en dat de resultaten ervan moeten worden gebruikt om de in artikel 6 bedoelde risicobeoordeling van de financiële entiteit bij te werken.

4. In het beleid worden de passende maatregelen vastgesteld die de financiële entiteit moet nemen indien zij tekortkomingen vaststelt van de derde aanbieders van ICT-diensten, met inbegrip van ICT-gerelateerde incidenten en operationele of beveiligingsbetalingsincidenten, bij de verlening van de ICT-diensten ter ondersteuning van kritieke of belangrijke functies of bij de naleving van contractuele overeenkomsten of wettelijke vereisten. In het beleid wordt ook gespecificeerd hoe de uitvoering van dergelijke maatregelen moet worden gemonitord om ervoor te zorgen dat zij binnen een bepaalde termijn daadwerkelijk worden nageleefd, rekening houdend met het relatieve belang van de tekortkomingen.

Artikel 10

Exit uit en beëindiging van de contractuele overeenkomsten:

Het beleid moet vereisten bevatten voor een gedocumenteerd exitplan voor elke contractuele overeenkomst en voor de periodieke evaluatie en toetsing van het gedocumenteerde exitplan. Bij het opstellen van het exitplan wordt rekening gehouden met het volgende:

(a) onvoorziene en aanhoudende onderbrekingen van de dienstverlening;

(b) ongeschikte of falende dienstverlening;

(c) onverwachte beëindiging van de contractuele overeenkomst.

Het exitplan is realistisch en haalbaar, is gebaseerd op plausibele scenario's en redelijke veronderstellingen en heeft een geplande uitvoeringstiming die verenigbaar is met de in de contractuele overeenkomst vastgestelde exit- en beëindigingsvoorwaarden.

Artikel 11

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 13 maart 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN