Publicatieblad
van de Europese Unie

NL
L-serie

2025/295

13.2.2025

GEDELEGEERDE VERORDENING (EU) 2025/295 VAN DE COMMISSIE

van 24 oktober 2024

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen voor de harmonisatie van de voorwaarden voor de uitoefening van de oversightactiviteiten

(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 41, lid 2, tweede alinea,

Overwegende hetgeen volgt:

(1) Bij het kader inzake digitale operationele weerbaarheid voor de financiële sector dat is opgezet bij Verordening (EU) 2022/2554, wordt een Unie-oversightkader ingevoerd voor derde aanbieders van diensten van informatie- en communicatietechnologie (ICT-diensten) aan de financiële sector die zijn aangewezen als cruciaal in overeenstemming met artikel 31 van die verordening.

(2) Een derde aanbieder van ICT-diensten die besluit een vrijwillig verzoek in te dienen om te worden aangewezen als cruciaal, moet de Europese toezichthoudende autoriteit (ETA) die dit verzoek ontvangt, alle nodige informatie verstrekken waaruit blijkt dat deze een kritieke ICT-dienstverlener is volgens de beginselen en criteria van Verordening (EU) 2022/2554. Derhalve moet de in het vrijwillige verzoek op te nemen informatie gedetailleerd en volledig genoeg zijn om een duidelijke en volledige beoordeling van het kritieke karakter van de aanbieder uit hoofde van artikel 31, lid 11, van die verordening mogelijk te maken. De desbetreffende ETA moet onvolledige verzoeken weigeren en om de ontbrekende informatie verzoeken.

(3) Voor de juridische aanduiding van derde aanbieders van ICT-diensten binnen het toepassingsgebied van deze technische reguleringsnormen moet gebruik worden gemaakt van de identificatiecode uit de uitvoeringsverordening van de Commissie die in overeenstemming met artikel 28, lid 9, van Verordening (EU) 2022/2554 is vastgesteld.

(4) In vervolg op de aanbevelingen van de lead overseer aan kritieke derde aanbieders van ICT-diensten moet de lead overseer de naleving, door de kritieke derde aanbieders van ICT-diensten, van de aanbevelingen monitoren. Voor een doelmatige en doeltreffende monitoring van de actie die is ondernomen of corrigerende maatregelen die zijn getroffen door kritieke derde aanbieders van ICT-diensten in verband met deze aanbevelingen, moet de lead overseer kunnen verzoeken om de in artikel 35, lid 1, punt c), van Verordening (EU) 2022/2554 bedoelde verslagen, waaronder tussentijdse voortgangsverslagen en eindverslagen moeten worden verstaan.

(5) In het kader van de beoordeling uit hoofde van artikel 42, lid 1, van Verordening (EU) 2022/2554, volgens welk de lead overseer moet evalueren of de motivatie van de kritieke derde aanbieder van ICT-diensten toereikend is, moet de kennisgeving, aan de lead overseer, van de kritieke derde aanbieder van ICT-diensten van diens voornemen om de ontvangen aanbevelingen op te volgen, worden aangevuld met een beschrijving van de ondernomen actie en genomen maatregelen om de in de aanbevelingen geschetste risico's te beperken, samen met de respectieve termijnen daarvoor. Een dergelijke motivatie moet de vorm aannemen van een correctieplan.

(6) Omdat van de lead overseer wordt verwacht dat deze de onderaannemingsovereenkomsten van de kritieke derde aanbieder van ICT-diensten beoordeelt, moet een model worden ontwikkeld voor de verstrekking van informatie over dergelijke regelingen. Voor dit model moet rekening worden gehouden met het feit dat kritieke derde aanbieders van ICT-diensten een andere structuur hebben dan financiële entiteiten.

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

(7) Nadat de lead overseer een kritieke derde aanbieder van ICT-diensten aanbevelingen heeft gedaan en de bevoegde autoriteiten de relevante financiële entiteiten op de hoogte hebben gebracht van de risico's die in die aanbevelingen zijn geconstateerd, moet de lead overseer de uitvoering door de kritieke derde aanbieder van ICT-diensten van de acties en corrigerende maatregelen om aan de aanbevelingen te voldoen, monitoren en beoordelen. De bevoegde autoriteiten moeten monitoren en beoordelen in hoeverre de financiële entiteiten zijn blootgesteld aan de in deze aanbevelingen geconstateerde risico's. Met het oog op het behoud van een gelijk speelveld bij de uitvoering van hun respectieve taken, met name wanneer de in de aanbevelingen geconstateerde risico's ernstig zijn en een groot aantal financiële entiteiten in meerdere lidstaten raken, moeten zowel de bevoegde autoriteiten als de lead overseer onderling relevante bevindingen uitwisselen die nodig zijn voor de uitvoering van hun respectieve taken. De informatie-uitwisseling heeft tot doel ervoor te zorgen dat in de feedback van de lead overseer aan de kritieke derde aanbieder van ICT-diensten over de acties en corrigerende maatregelen die deze laatste uitvoert, rekening wordt gehouden met de gevolgen voor de risico's van de financiële entiteiten, en dat de beoordeling van de lead overseer als input dient voor de toezichtactiviteiten van de bevoegde autoriteiten.

(8) Om een doelmatige en doeltreffende informatie-uitwisseling mogelijk te maken, moeten de bevoegde autoriteiten in het kader van hun toezichtactiviteiten beoordelen in hoever de financiële entiteiten waarop zij toezicht houden, zijn blootgesteld aan de in de aanbevelingen gesignaleerde risico's. Deze beoordeling moet op evenredige wijze worden uitgevoerd en risicogebaseerd zijn. Ingeval de in de aanbevelingen gesignaleerde risico's ernstig zijn en een groot aantal financiële entiteiten in meerdere lidstaten raken, moet de lead overseer van de bevoegde autoriteiten de resultaten van deze beoordeling opvragen bij de bevoegde autoriteiten. Om een optimale benutting van de middelen van bevoegde autoriteiten te waarborgen, moet de lead overseer die om de resultaten van de beoordeling verzoekt, er telkens rekening mee houden dat deze verzoeken bedoeld zijn voor de evaluatie van de uitvoering van acties en corrigerende maatregelen van de kritieke derde aanbieders van ICT-diensten.

(9) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([2]) en heeft op 22 juli 2024 een advies uitgebracht.

(10) Deze verordening berust op de ontwerpen van technische reguleringsnormen die de ETA's bij de Commissie hebben ingediend.

(11) Het Gemengd Comité van de ETA's heeft openbare raadplegingen gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, de mogelijke kosten en baten ervan geanalyseerd en het advies ingewonnen van de overeenkomstig artikel 37 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([3]) opgerichte Stakeholdergroep bankwezen, van de overeenkomstig artikel 37 van Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([4]) opgerichte Stakeholdergroep verzekeringen en herverzekeringen en Stakeholdergroep bedrijfspensioenen, en van de overeenkomstig artikel 37 van Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad ([5]) opgerichte Stakeholdergroep effecten en markten,

([2]) 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).

([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).

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Informatie die derde aanbieders van ICT-diensten moeten verstrekken in hun verzoek om te worden aangewezen als cruciaal

1. De derde aanbieders van diensten van informatie- en communicatietechnologie (ICT-diensten) dient in het met redenen omklede vrijwillige verzoek uit hoofde van artikel 31, lid 11, van Verordening (EU) 2022/2554 om te worden aangewezen als cruciaal in overeenstemming met artikel 31, lid 1, punt a), van Verordening (EU) 2022/2554, de volgende informatie in:

a) naam van de rechtspersoon;

b) identificatiecode van de rechtspersoon;

c) naam van de contactpersoon en contactgegevens van de kritieke derde aanbieder van ICT-diensten;

d) land van de maatschappelijke zetel van de rechtspersoon;

e) beschrijving van de structuur van de onderneming, met ten minste informatie over de moedermaatschappij en andere verwante ondernemingen die ICT-diensten verlenen aan financiële entiteiten in de Unie. In voorkomend geval omvat deze informatie:

   i) naam van de rechtspersonen;

   ii) identificatiecode van de rechtspersoon;

   iii) land van de maatschappelijke zetel van de rechtspersoon;

f) een raming van het marktaandeel van de derde aanbieder van ICT-diensten in de financiële sector van de Unie en een raming van het marktaandeel per soort financiële entiteit als bedoeld in artikel 2, lid 1, van Verordening (EU) 2022/2554, voor het jaar van indiening van het verzoek om te worden aangewezen als cruciaal, en voor het jaar vóór indiening van dat verzoek;

g) een beschrijving van elke ICT-dienst die wordt verleend aan financiële entiteiten in de Unie, met inbegrip van:

   i) een beschrijving van de aard van de zakelijke relatie en de soort ICT-diensten die aan financiële entiteiten wordt verleend;

   ii) indien beschikbaar, een lijst van de functies van financiële entiteiten die worden ondersteund met de verleende ICT-diensten;

   iii) indien beschikbaar, informatie over de vraag of de aan financiële entiteiten verleende ICT-diensten kritieke of belangrijke functies ondersteunen;

h) een lijst van financiële entiteiten die gebruikmaken van ICT-diensten van de derde aanbieder van ICT-diensten, met inbegrip van de volgende informatie voor elk van de bediende financiële entiteiten, indien beschikbaar:

   i) naam van de rechtspersoon;

   ii) identificatiecode van de rechtspersoon, indien bekend bij de derde aanbieder van ICT-diensten;

   iii) soort financiële entiteit overeenkomstig artikel 2, lid 1, van Verordening (EU) 2022/2554;

   iv) de geografische locatie vanwaaruit de ICT-diensten aan die rechtspersoon worden verleend;

i) een lijst met de kritieke derde aanbieders van ICT-diensten die zijn opgenomen in de meest recente beschikbare lijst van dergelijke aanbieders die overeenkomstig artikel 31, lid 9, van Verordening (EU) 2022/2554 door de ETA's wordt gepubliceerd;

j) een zelfbeoordeling met betrekking tot de volgende aspecten:

   i) de mate van substitueerbaarheid van elke ICT-dienst van de verzoeker, met inachtneming van het volgende:

      — het marktaandeel van de derde aanbieder van ICT-diensten in de financiële sector van de Unie;

— het aantal bekende relevante concurrenten per soort ICT-dienst of per groep ICT-diensten;

— beschrijving van de specifieke kenmerken van de aangeboden ICT-diensten, onder meer met betrekking tot bedrijfseigen technologieën, of de specifieke kenmerken van de organisatie of activiteit van de derde aanbieder van ICT-diensten;

ii) bekende beschikbare alternatieve derde aanbieders van ICT-diensten die dezelfde ICT-diensten verlenen als de derde aanbieder van ICT-diensten die het verzoek indient;

k) informatie over een toekomstige bedrijfsstrategie met betrekking tot de verlening van ICT-diensten en -infrastructuur aan financiële entiteiten in de Unie, met inbegrip van eventuele geplande wijzigingen in de groeps- of beheerstructuur, de betreding van nieuwe markten of de ontwikkeling van nieuwe activiteiten;

l) vermelding van de subcontractanten van de derde aanbieder van ICT-diensten die zijn aangewezen als kritieke derde aanbieders van ICT-diensten;

m) andere aspecten die van belang zijn voor het verzoek van de derde aanbieder van ICT-diensten om te worden aangewezen als cruciaal.

2. Indien de derde aanbieder van ICT-diensten tot een groep behoort, wordt de in lid 1 bedoelde informatie verstrekt voor de ICT-diensten die door de groep als geheel worden verleend.

Artikel 2

Inhoud, structuur en formaat van de informatie die kritieke derde aanbieders van ICT-diensten moeten indienen, bekendmaken of rapporteren

1. Kritieke derde aanbieders van ICT-diensten verstrekken de lead overseer die daarom verzoekt, alle informatie die deze nodig heeft voor de uitvoering van diens oversighttaken overeenkomstig Verordening (EU) 2022/2554.

2. De in lid 1 bedoelde informatie omvat onder meer:

a) informatie over de regelingen, en kopieën van contractuele documenten, tussen:

i) de kritieke derde aanbieder van ICT-diensten en de in artikel 2, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten;

ii) de kritieke derde aanbieder van ICT-diensten en de subcontractanten van deze aanbieder, voor inzicht in de technologische waardeketen van de ICT-diensten die worden verleend aan financiële entiteiten in de Unie;

b) informatie over de organisatie- en groepsstructuur van de kritieke derde aanbieder van ICT-diensten, met vermelding van alle entiteiten die tot dezelfde groep behoren en die direct of indirect ICT-diensten verlenen aan financiële entiteiten in de Unie;

c) informatie over de belangrijkste aandeelhouders, met inbegrip van hun structuur en geografische distributie, voor alle onderstaande entiteiten:

i) entiteiten die, alleen of samen met aan hen gelieerde entiteiten, 25 % of meer van het kapitaal van of de stemrechten binnen de kritieke derde aanbieder van ICT-diensten bezitten;

ii) entiteiten die het recht hebben om een meerderheid van de leden van het bestuurlijke, beleidsbepalende of toezichthoudende orgaan van de kritieke derde aanbieder van ICT-diensten te benoemen of ontslaan;

iii) entiteiten die op grond van een overeenkomst zeggenschap hebben over een meerderheid van de stemrechten van aandeelhouders of leden van de kritieke derde aanbieder van ICT-diensten;

d) informatie over het marktaandeel van de kritieke derde aanbieder van ICT-diensten per soort dienst, in de relevante markten waar deze actief is;

e) informatie over de interne governanceregelingen van de kritieke derde aanbieder van ICT-diensten, met inbegrip van de structuur met regels inzake taakverdeling en verantwoording;

f) de notulen van vergaderingen van het leidinggevend orgaan en andere interne relevante comités die op enigerlei wijze betrekking hebben op activiteiten en risico's betreffende ICT-diensten van derden die functies van financiële entiteiten in de Unie ondersteunen;

g) informatie over de ICT-beveiliging van de kritieke derde aanbieder van ICT-diensten, met inbegrip van relevant(e) strategieën, doelstellingen, beleid, procedures, protocollen, processen, controlemaatregelen om gevoelige gegevens te beschermen, toegangscontroles, versleutelingspraktijken, incidentresponsplannen en, in voorkomend geval, informatie over de naleving van alle relevante voorschriften en nationale en internationale normen;

h) informatie over technische en organisatorische maatregelen om de bescherming en vertrouwelijkheid van gegevens, met inbegrip van persoonsgegevens en niet-persoonsgebonden gegevens, te waarborgen en over ingevoerde controlemaatregelen om gevoelige gegevens te beschermen, toegangscontroles, versleutelingspraktijken en een responsplan voor datalekken; indien de derde aanbieder van ICT-diensten met betrekking tot de verwerking van persoonsgegevens is onderworpen aan wetten van derde landen, met inbegrip van toegangsverzoeken van overheden van derde landen, een lijst met landen en de toepasselijke wetgeving;

i) informatie over de mechanismen die de kritieke derde aanbieder van ICT-diensten financiële entiteiten in de Unie aanbiedt voor de overdracht van gegevens en applicaties en interoperabiliteit;

j) informatie over de locatie van de datacenters en ICT-productiecentra die worden gebruikt om diensten te verlenen aan financiële entiteiten, met inbegrip van een lijst van alle relevante bedrijfsruimten en voorzieningen van de kritieke derde aanbieder van ICT-diensten, ook die buiten de Unie;

k) informatie over de verlening van diensten door de kritieke derde aanbieder van ICT-diensten vanuit derde landen, met inbegrip van informatie over relevante wettelijke bepalingen inzake persoonsgegevens en niet-persoonsgebonden gegevens die door de aanbieder van ICT-diensten worden verwerkt;

(l) informatie over de genomen maatregelen om risico's te adresseren die voortvloeien uit de verlening van ICT-diensten vanuit derde landen door de kritieke derde aanbieder van ICT-diensten en diens subcontractanten;

m) informatie over het kader voor risicobeheer en het kader voor incidentbeheer, met inbegrip van beleid, procedures, hulpmiddelen, mechanismen en governanceregelingen van de kritieke derde aanbieder van ICT-diensten en van diens subcontractanten, met inbegrip van een lijst en beschrijving van belangrijke incidenten met directe of indirecte gevolgen voor financiële entiteiten in de Unie, inclusief nadere informatie op basis waarvan de significantie van het incident voor financiële entiteiten kan worden bepaald en eventuele grensoverschrijdende gevolgen kunnen worden beoordeeld;

n) informatie over het kader voor veranderingsbeheer, met inbegrip van beleid, procedures en controles, van de kritieke derde aanbieder van ICT-diensten en diens subcontractanten;

o) informatie over het algehele respons- en herstelkader van de kritieke derde aanbieder van ICT-diensten, met inbegrip van bedrijfscontinuïteitsplannen en verwante regelingen en procedures, levenscyclusbeleid met betrekking tot softwareontwikkeling, respons- en herstelplannen en verwante regelingen en procedures, en beleid, regelingen en procedures inzake back-ups;

p) informatie over prestatiebewaking, beveiligingsbewaking en het volgen van incidenten, alsmede informatie over rapportagemechanismen met betrekking tot de prestaties van diensten, incidenten en naleving van overeengekomen dienstenniveauovereenkomsten (SLA's) en doelstellingen inzake dienstverleningsniveau, of vergelijkbare regelingen tussen kritieke derde aanbieders van ICT-diensten en financiële entiteiten in de Unie;

q) informatie over het voor ICT-derden opgezette beheerskader van de kritieke derde aanbieder van ICT-diensten, met inbegrip van strategieën, beleid, procedures, processen en controles, inclusief nadere informatie over de vooronderzoeken en risicobeoordelingen die de kritieke derde aanbieder van ICT-diensten ten aanzien van diens subcontractanten uitvoert voordat een overeenkomst met hen wordt aangegaan, teneinde de relatie te bewaken voor alle relevante ICT-risico's en met de wederpartij samenhangende risico's;

r) uittreksels uit de bewakings- en scansystemen van de kritieke derde aanbieder van ICT-diensten en diens subcontractanten, onder meer — maar niet uitsluitend — met betrekking tot netwerk-, server-, applicatie- en beveiligingsbewaking, kwetsbaarheidsscans, beheer van logboeken, prestatiebewaking, incidentbeheer en toetsingen aan betrouwbaarheidsdoelstellingen, zoals doelstellingen inzake dienstverleningsniveau;

s) uittreksels uit productie-, preproductie- en testsystemen of -applicaties die de kritieke derde aanbieder van ICT-diensten en diens subcontractanten gebruiken om direct of indirect diensten te verlenen aan financiële entiteiten in de Unie;

t) conformiteits- en beschikbare auditverslagen, evenals relevante auditbevindingen, met inbegrip van audits die zijn uitgevoerd door nationale autoriteiten in de Unie en buiten de Unie, indien samenwerkingsovereenkomsten met de desbetreffende autoriteiten voorzien in een dergelijke informatie-uitwisseling, of certificeringen die zijn verkregen door de kritieke derde aanbieder van ICT-diensten of diens subcontractanten, met inbegrip van verslagen van interne en externe auditoren, certificeringen, of toetsingen op de conformiteit met branchespecifieke normen. Daaronder valt ook informatie over elk type beschikbare onafhankelijke tests van de weerbaarheid van de ICT-systemen van de kritieke derde aanbieder van ICT-diensten, met inbegrip van elk type op bedreigingen gebaseerde penetratietests die de derde aanbieder van ICT-diensten heeft uitgevoerd;

u) informatie over door de kritieke derde aanbieder van ICT-diensten op diens verzoek of in diens naam verrichte beoordelingen van de geschiktheid en integriteit van personen die sleutelposities binnen de kritieke derde aanbieder van ICT-diensten bekleden;

v) informatie over correctieplannen naar aanleiding van aanbevelingen uit hoofde van artikel 3 en relevante verwante informatie waaruit blijkt dat corrigerende maatregelen zijn getroffen;

w) informatie over voor het personeel beschikbare opleidingsprogramma's en bewustmakingsprogramma's op het gebied van beveiliging, waaronder, waar relevant, informatie over investeringen, middelen en methoden van de kritieke derde aanbieder van ICT-diensten met betrekking tot de opleiding van diens personeel in de behandeling van gevoelige financiële gegevens en in de wijze waarop de beveiliging op een hoog peil kan worden gehouden;

x) informatie over de activiteiten van de kritieke derde aanbieder van ICT-diensten en financiële overzichten, met inbegrip van informatie over de begroting en middelen voor ICT en beveiliging.

Artikel 3

Informatie van kritieke derde aanbieders van ICT-diensten nadat aanbevelingen zijn gedaan

1. De kritieke derde aanbieder van ICT-diensten levert de lead overseer een verslag met een correctieplan met betrekking tot de aanbevelingen, waarin wordt aangegeven welke corrigerende maatregelen de kritieke derde aanbieder van ICT-diensten voornemens is te treffen om de risico's te beperken die zijn geconstateerd in de aanbevelingen als bedoeld in artikel 35, lid 1, punt d), van Verordening (EU) 2022/2254. Het verslag volgt de termijnen die de lead overseer heeft gesteld voor elke aanbeveling.

2. Om de lead overseer in staat te stellen om de uitvoering te monitoren van de actie en corrigerende maatregelen die de kritieke derde aanbieder van ICT-diensten naar aanleiding van de ontvangen aanbevelingen heeft ondernomen en getroffen, deelt de kritieke derde aanbieder van ICT-diensten op verzoek de volgende documenten met de lead overseer:

a) tussentijdse voortgangsverslagen en verwante ondersteunende documenten over de vorderingen bij de uitvoering van de acties en maatregelen die zijn vermeld in het verslag dat de kritieke derde aanbieder van ICT-diensten binnen de door de lead overseer gestelde tijdlijn aan de lead overseer heeft verstrekt;

b) eindverslagen en verwante ondersteunende documentatie over de actie die de kritieke derde aanbieder van ICT-diensten heeft ondernomen en de corrigerende maatregelen die deze heeft getroffen om de in de ontvangen aanbevelingen geconstateerde risico's te beperken.

Artikel 4

Structuur en formaat van de informatie van kritieke derde aanbieders van ICT-diensten

1. De kritieke derde aanbieder van ICT-diensten verstrekt de lead overseer de gevraagde informatie via de door de lead overseer in diens verzoek aangegeven speciale veilige elektronische kanalen en in de door de lead overseer aangegeven vorm.

2. Bij het verstrekken van informatie aan de lead overseer moeten de kritieke derde aanbieders van ICT-diensten:

a) de structuur volgen die de lead overseer heeft aangegeven in diens verzoek om informatie;

b) duidelijk aangeven waar de relevante informatie-elementen in de ingediende documentatie te vinden zijn.

3. De informatie die de kritieke derde aanbieder van ICT-diensten bij of aan de lead overseer indient, bekendmaakt of rapporteert, is gesteld in een in internationale financiële kringen gebruikelijke taal.

Artikel 5

Model voor het verstrekken van informatie over onderaannemingsovereenkomsten

Een kritieke derde aanbieder van ICT-diensten die informatie over onderaannemingsovereenkomsten moet delen, verstrekt deze informatie aan de lead overseer volgens het model van de bijlage.

Artikel 6

Beoordeling door de bevoegde autoriteiten van de risico's die zijn geadresseerd in de aanbevelingen van de lead overseer

1. In het kader van haar toezicht op financiële entiteiten beoordeelt de bevoegde autoriteit de gevolgen voor financiële entiteiten van de maatregelen die de kritieke derde aanbieder van ICT-diensten heeft genomen op basis van de aanbevelingen van de lead overseer, in overeenstemming met het evenredigheidsbeginsel.

2. Bij de in lid 1 bedoelde beoordeling houdt de bevoegde autoriteit rekening met:

a) de toereikendheid van en samenhang tussen de corrigerende maatregelen van de financiële entiteiten om de in de aanbevelingen geconstateerde risico's te beperken;

b) de beoordeling door de lead overseer van de naleving, door de kritieke derde aanbieder van ICT-diensten, van de maatregelen en acties die zijn vermeld in het verslag, wanneer deze beoordeling gevolgen heeft voor de blootstelling van de onder haar bevoegdheid vallende financiële entiteiten aan de in de aanbevelingen geconstateerde risico's;

c) de standpunten van andere bevoegde autoriteiten die zijn geraadpleegd in overeenstemming met artikel 42, lid 5, van Verordening (EU) 2022/2554;

d) de vraag of de lead overseer de acties en corrigerende maatregelen van de kritieke derde aanbieder van ICT-diensten toereikend acht om de blootstelling van de onder haar bevoegdheid vallende financiële entiteiten aan de in de aanbeveling geconstateerde risico's te beperken.

3. Op verzoek van de lead overseer verschaft de bevoegde autoriteit de resultaten van de in lid 1 bedoelde beoordeling binnen een redelijke termijn. Bij het opvragen van de resultaten van deze beoordeling neemt de lead overseer het evenredigheidsbeginsel en de omvang van de in de aanbevelingen geconstateerde risico's in acht, met inbegrip van de grensoverschrijdende gevolgen van deze risico's wanneer ze financiële entiteiten in meer dan een lidstaat raken.

4. Waar relevant verzoekt de bevoegde autoriteit financiële entiteiten de informatie te verstrekken die nodig is voor de uitvoering van de in lid 1 bedoelde beoordeling.

Artikel 7

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, 24 oktober 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE

MODEL VOOR HET DELEN VAN INFORMATIE OVER ONDERAANNEMINGSOVEREENKOMSTEN

Informatiecategorie	Belangrijkste informatie-elementen
Algemene informatie	— Naam van de kritieke derde aanbieder van ICT-diensten. — Identificatiecode van de kritieke derde aanbieder van ICT-diensten. — Naam van de contactpersoon en contactgegevens van de kritieke derde aanbieder van ICT-diensten. — Datum van indiening van het model.
Overzicht van onderaannemingsovereenkomsten	— Overzicht van de onderaannemingsovereenkomsten, met inbegrip van een korte beschrijving van het doeleinde en toepassingsgebied van de onderaannemingsrelaties (waarin ook wordt aangegeven in welke mate de onderaannemingsovereenkomsten van kritieke aard of van belang zijn voor de kritieke derde aanbieder van ICT-diensten). — Uitsplitsing en beschrijving van de soorten ICT-diensten die in onderaanneming zijn gegeven, en het belang ervan voor de ICT-diensten die worden verleend aan financiële entiteiten, in overeenstemming met de technische uitvoeringsnormen die zijn vastgesteld in het kader van artikel 28, lid 9, van Verordening (EU) 2022/2554. — Gelieve bij het opgeven van de soorten ICT-diensten de lijst te raadplegen in bijlage IV bij de technische uitvoeringsnormen die zijn vastgesteld in het kader van artikel 28, lid 9, van Verordening (EU) 2022/2554.
Informatie over de subcontractanten	— Naam en gegevens van de rechtspersoon (met identificatiecode) voor elke subcontractant. — Contactgegevens van de personeelsleden die in de beheersstructuur van de kritieke derde aanbieder van ICT-diensten verantwoordelijk zijn voor de relatie met elke subcontractant. — Overzicht van de deskundigheid, ervaring en kwalificaties met betrekking tot de aanbestede ICT-diensten voor elke subcontractant.
Beschrijving van de diensten van subcontractanten	— Gedetailleerde beschrijving van de specifieke ICT-diensten van elke subcontractant. — Uitsplitsing van de verantwoordelijkheden en taken die zijn toegewezen aan subcontractanten, in de vorm van een gedetailleerde toelichting van de verschillende rollen in de verschillende stadia van de ICT-processen. — Informatie over het niveau van toegang die subcontractanten hebben tot persoonsgegevens of andere gevoelige gegevens of systemen in het kader van de ICT-diensten die aan financiële entiteiten worden verleend. — Informatie over de locaties vanwaaruit de diensten van subcontractanten worden verleend, en over de genomen maatregelen om de risico's te adresseren die voortvloeien uit diensten die buiten de Unie worden verleend.
Governance en toezicht — subcontractanten	— Beschrijving van het bestaande contractuele en governancekader voor onderaannemingsrelaties, met inbegrip van clausules ter beperking van het gebruik van gevoelige gegevens. — Toelichting van de processen voor de selectie van, interactie met en monitoring van subcontractanten. — Overzicht van prestatiemaatstaven, doelstellingen en overeenkomsten inzake dienstverleningsniveau, en kernprestatie-indicatoren voor de bewaking van de prestaties en betrouwbaarheid van subcontractanten.
Risicobeheer en naleving	— Beoordeling van de risicoprofielen van subcontractanten en potentiële gevolgen voor de ICT-diensten die aan financiële entiteiten worden verleend. — Toelichting van de getroffen risicobeperkende maatregelen om risico's te adresseren die verband houden met subcontractanten. — Nadere informatie over de naleving door subcontractanten van relevante regelgeving, met inbegrip van regelgeving inzake gegevensbescherming en branchenormen.

Informatiecategorie	Belangrijkste informatie-elementen
Bedrijfscontinuïteits- en noodplannen	— Overzicht van de bedrijfscontinuïteits- en respons- en herstelplannen van subcontractanten. — Beschrijving van de bestaande regelingen om de continuïteit van de dienst te waarborgen in het geval van storingen bij of beëindiging door de subcontractant. — Regelmaat waarmee subcontractanten hun bedrijfscontinuïteitsplannen en respons- en herstelplannen testen, datums van de laatste tests in de afgelopen drie jaar en vermelding of de kritieke derde aanbieder van ICT-diensten bij deze tests was betrokken.
Verslaglegging	— Beschrijving van de mechanismen voor en regelmaat van rapportage tussen de kritieke derde aanbieder van ICT-diensten en diens subcontractanten.
Correctie en incidentbeheer	— Overzicht van de procedures voor het adresseren van subcontractantgerelateerde incidenten, inbreuken of gevallen van niet-naleving.
Certificeringen en audits	— Informatie over certificeringen en over uitgevoerde onafhankelijke audits en beoordelingen van de beveiligingscontroles en kwaliteitsnormen van en de naleving van de regelgeving door subcontractanten. — Datum en regelmaat van de door de kritieke derde aanbieder van ICT-diensten verrichte audits van de subcontractanten.