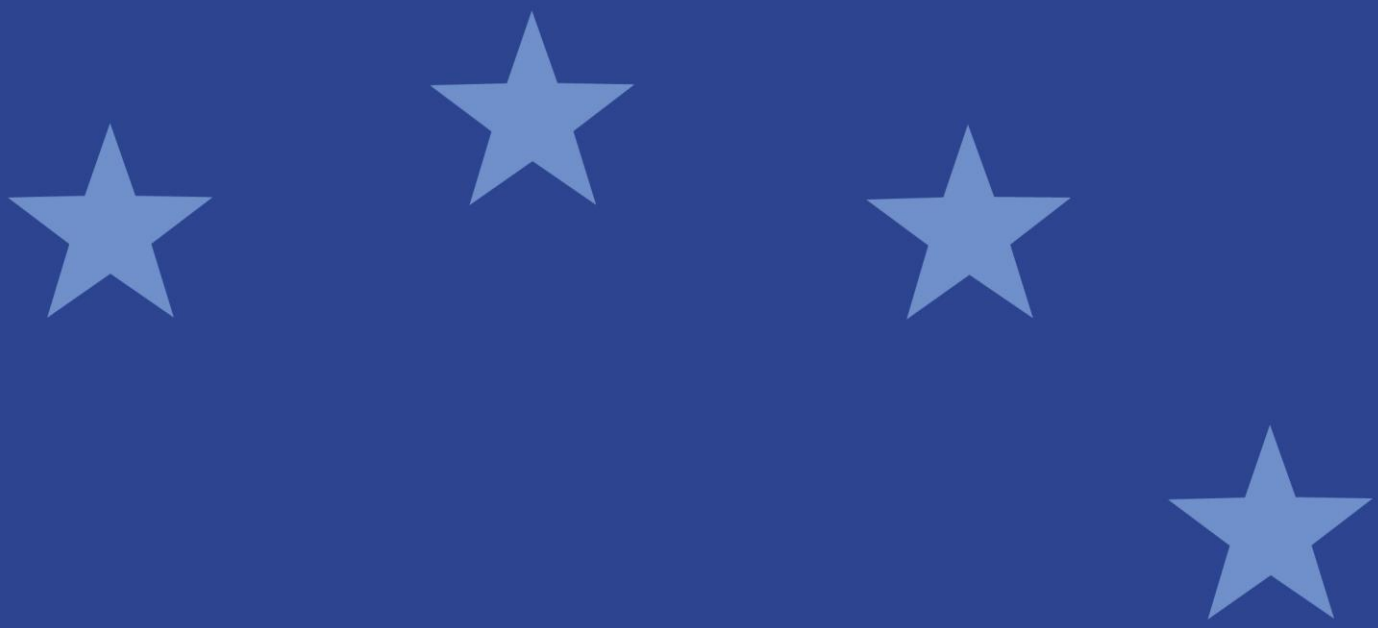
esma European Securities and Markets Authority

Richtsnoeren

inzake uitbesteding aan aanbieders van clouddiensten



10/05/2021 | ESMA50-164-4285 NL

Inhoudsopgave

I. Toepassingsgebied 2
II. Wettelijke verwijzingen, afkortingen en definities 3
III. Doel 10
IV. Verplichtingen inzake naleving en rapportage 10
V. Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten 11
Richtsnoer 1. Governance, toezicht en documentatie 11
Richtsnoer 2. Analyse voorafgaand aan uitbesteding en due diligence 13
Richtsnoer 3. Essentiële contractuele bepalingen 15
Richtsnoer 4. Informatiebeveiliging 17
Richtsnoer 5. Exitstrategieën 18
Richtsnoer 6. Toegangs- en auditrecht 19
Richtsnoer 7. Onderuitbesteding 21
Richtsnoer 8. Schriftelijke kennisgeving aan bevoegde autoriteiten 22
Richtsnoer 9. Toezicht op uitbestedingsovereenkomsten voor clouddiensten 23

I. Toepassingsgebied

Wie?

1. Deze richtsnoeren gelden voor bevoegde autoriteiten en voor i) beheerders van alternatieve beleggingsinstellingen (abi-beheerders) en bewaarders van alternatieve beleggingsinstellingen (abi's), ii) instellingen voor collectieve belegging in effecten (icbe's), beheermaatschappijen en bewaarders van icbe's, en beleggingsmaatschappijen die geen beheermaatschappij hebben aangesteld waaraan krachtens de icbe-richtlijn vergunning is verleend, iii) centrale tegenpartijen (CTP's), waaronder tier 2-CTP's uit derde landen die voldoen aan de relevante EMIR-voorschriften, iv) transactieregisters (TR's), v) beleggingsondernemingen en kredietinstellingen bij het verlenen van beleggingsdiensten en het verrichten van beleggingsactiviteiten, aanbieders van datarapporteringsdiensten en marktexploitanten van handelsplatformen, vi) centrale effectenbewaarinstellingen (CSD's), vii) ratingbureaus (RB's), viii) securitisatieregisters (SR's) en ix) beheerders van cruciale benchmarks.

2. ESMA zal deze richtsnoeren tevens in acht nemen bij haar beoordeling van de mate waarin een tier 2-CTP uit een derde land aan de relevante EMIR-voorschriften voldoet door naleving van vergelijkbare voorschriften in het derde land overeenkomstig artikel 25, lid 2 ter, onder a), van EMIR.

Wat?

3. Deze richtsnoeren zijn van toepassing in verband met de volgende bepalingen:

   a) de artikelen 15, 18 en 20 en artikel 21, lid 8, van de AIFM-richtlijn; de artikelen 13, 22, 38, 39, 40, 44 en 45, artikel 57, lid 1, onder d), en leden 2 en 3, en de artikelen 58, 75, 76, 77, 79, 81, 82 en 98 van Gedelegeerde Verordening (EU) 231/2013 van de Commissie;
   b) artikel 12, lid 1, onder a), artikel 13, artikel 14, lid 1, onder c), artikel 22, artikel 22 bis, artikel 23, lid 2, en de artikelen 30 en 31 van de icbe-richtlijn; artikel 4, leden 1, 2, 3 en 5, artikel 5, lid 2, de artikelen 7 en 9, artikel 23, lid 4, en de artikelen 32, 38, 39 en 40 van Richtlijn 2010/43/EU van de Commissie; artikel 2, lid 2, onder j), artikel 3, lid 1, artikel 13, lid 2, en de artikelen 15, 16 en 22 van Gedelegeerde Verordening (EU) 2016/438 van de Commissie;
   c) artikel 25, artikel 26, leden 1, 3 en 6, de artikelen 34, 35 en 78 tot en met 81 van de verordening betreffende de Europese marktinfrastructuur (EMIR); de artikelen 5 en 12 van de SFTR-verordening; artikel 3, lid 1, onder f), en leden 2 en 4, artikel 7, lid 2, onder d) en f), en de artikelen 9 en 17 van Gedelegeerde Verordening (EU) nr. 153/2013 van de Commissie; de artikelen 16 en 21 van Gedelegeerde Verordening (EU) nr. 150/2013 van de Commissie; de artikelen 16 en 21 van Gedelegeerde Verordening (EU) 2019/359 van de Commissie;

d) artikel 16, leden 2, 4 en 5, artikel 18, lid 1, artikel 19, lid 3, onder a), artikel 47, lid 1, onder b) en c), artikel 48, lid 1, artikel 64, lid 4, artikel 65, lid 5, en artikel 66, lid 31 van MiFID II; artikel 21, leden 1 tot en met 3, artikel 23, artikel 29, lid 5, en de artikelen 30, 31 en 32 van Gedelegeerde Verordening (EU) 2017/565 van de Commissie; de artikelen 6 en 15 en artikel 16, lid 6, van Gedelegeerde Verordening (EU) 2017/584 van de Commissie; de artikelen 6, 7, 8 en 9 van Gedelegeerde Verordening (EU) 2017/571 van de Commissie;
e) de artikelen 22, 26, 30, 42, 44 en 45 van de CSDR en de artikelen 33 en 47, artikel 50, lid 1, artikel 57, lid 2, onder i), en de artikelen 66, 68, 75, 76, 78 en 80 van Gedelegeerde Verordening (EU) 2017/392 van de Commissie;
f) artikel 9 en bijlage I, afdeling A, punten 4 en 8, en bijlage II, punt 17, bij de RB-verordening en de artikelen 11 en 25 van Gedelegeerde Verordening (EU) 2012/449 van de Commissie;
g) artikel 10, lid 2, van de securitisatieverordening;
h) artikel 6, lid 3, en artikel 10 van de benchmarkverordening en punt 7 van bijlage I bij Gedelegeerde Verordening (EU) 2018/1646 van de Commissie.

Wanneer?

4. Deze richtsnoeren gelden met ingang van 31 juli 2021 voor alle uitbestedingsovereenkomsten betreffende clouddiensten die op of na deze datum van kracht worden, verlengd worden of worden gewijzigd. Ondernemingen moeten bestaande uitbestedingsovereenkomsten betreffende clouddiensten dienovereenkomstig herzien en wijzigen om te zorgen dat zij uiterlijk op 31 december 2022 aan deze richtsnoeren voldoen. Wanneer de herziening van uitbestedingsovereenkomsten betreffende clouddiensten in verband met kritieke of belangrijke functies niet op 31 december 2022 is afgerond, moet de onderneming haar bevoegde autoriteit daarvan op de hoogte stellen, met vermelding van de maatregelen die zij heeft gepland om de herziening of de eventuele exitstrategie te voltooien.

II. Wettelijke verwijzingen, afkortingen en definities

Wetgeving waarnaar wordt verwezen

ESMA-verordening	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[2]

[1] Met ingang van 1 januari 2022 moet de verwijzing naar artikel 64, lid 4, artikel 65, lid 5, en artikel 66, lid 3, van MiFID II worden gelezen als verwijzing naar artikel 27 octies, lid 4, artikel 27 nonies, lid 5, en artikel 27 decies, lid 3, van MiFIR.
[2] PB L 331 van 15.12.2010, blz. 84.

AIFM-richtlijn	Richtlijn 2011/61/EU van het Europees Parlement en de Raad van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 1095/2010[3]
Gedelegeerde Verordening (EU) 231/2013 van de Commissie	Gedelegeerde Verordening (EU) 231/2013 van de Commissie van 19 december 2012 tot aanvulling van Richtlijn 2011/61/EU van het Europees Parlement en de Raad ten aanzien van vrijstellingen, algemene voorwaarden voor de bedrijfsuitoefening, bewaarders, hefboomfinanciering, transparantie en toezicht[4]
icbe-richtlijn	Richtlijn 2009/65/EG van het Europees Parlement en de Raad van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe's)[5]
Richtlijn 2010/43/EU van de Commissie	Richtlijn 2010/43/EU van de Commissie van 1 juli 2010 tot uitvoering van Richtlijn 2009/65/EG van het Europees Parlement en de Raad wat betreft organisatorische eisen, belangenconflicten, bedrijfsvoering, risicobeheer en inhoud van de overeenkomst tussen een bewaarder en een beheermaatschappij[6]
Gedelegeerde Verordening (EU) 2016/438 van de Commissie	Gedelegeerde Verordening (EU) 2016/438 van de Commissie van 17 december 2015 tot aanvulling van Richtlijn 2009/65/EG van het Europees Parlement en de Raad betreffende de verplichtingen van bewaarders[7]
EMIR	Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters[8]
SFTR	Verordening (EU) nr. 2015/2365 van het Europees Parlement en de Raad van 25 november 2015 betreffende de transparantie van effectenfinancieringstransacties en van hergebruik en tot wijziging van Verordening (EU) nr. 648/2012[9]
Gedelegeerde Verordening (EU) nr. 153/2013 van de Commissie	Gedelegeerde Verordening (EU) nr. 153/2013 van de Commissie van 19 december 2012 tot aanvulling van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad met betrekking tot technische

[3] PB L 174 van 1.7.2011, blz. 1.
[4] PB L 83 van 22.3.2013, blz. 1.
[5] PB L 302 van 17.11.2009, blz. 32.
[6] PB L 176 van 10.7.2010, blz. 42.
[7] PB L 78 van 24.3.2016, blz. 11.
[8] PB L 201 van 27.7.2012, blz. 1.
[9] PB L 337 van 23.12.2015, blz. 1.

	reguleringsnormen inzake vereisten voor centrale tegenpartijen[10]
Gedelegeerde Verordening (EU) nr. 150/2013 van de Commissie	Gedelegeerde Verordening (EU) nr. 150/2013 van de Commissie van 19 december 2012 tot aanvulling van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad betreffende otc-derivaten, centrale tegenpartijen en transactieregisters met technische reguleringsnormen tot nadere bepaling van de gegevens die in de aanvraag tot registratie als transactieregister moeten worden opgenomen[11]
Gedelegeerde Verordening (EU) 2019/359 van de Commissie	Gedelegeerde verordening (EU) 2019/359 van de Commissie van 13 december 2018 tot aanvulling van Verordening (EU) 2015/2365 van het Europees Parlement en de Raad ten aanzien van technische reguleringsnormen tot specificatie van de gegevens van de aanvraag tot registratie en uitbreiding van registratie als transactieregister[12]
MiFID II	Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU[13]
MiFIR	Verordening (EU) nr. 600/2014 van het Europees Parlement en de Raad betreffende markten in financiële instrumenten en tot wijziging van Verordening (EU) nr. 648/2012 ([14])
Gedelegeerde Verordening (EU) 2017/565 van de Commissie	Gedelegeerde Verordening (EU) 2017/565 van de Commissie van 25 april 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad wat betreft de door beleggingsondernemingen in acht te nemen organisatorische eisen en voorwaarden voor de bedrijfsuitoefening en wat betreft de definitie van begrippen voor de toepassing van genoemde richtlijn[15]
Gedelegeerde Verordening (EU) 2017/584 van de Commissie	Gedelegeerde Verordening (EU) 2017/584 van de Commissie van 14 juli 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen ter specificatie van de organisatorische vereisten voor handelsplatformen[16]

[10] PB L 52 van 23.2.2013, blz. 41.
[11] PB L 52 van 23.2.2013, blz. 25.
[12] PB L 81 van 22.3.2019, blz. 45.
[13] PB L 173 van 12.6.2014, blz. 349.
[14] PB L 173 van 12.6.2014, blz. 84.
[15] PB L 87 van 31.3.2017, blz. 1.
[16] PB L 87 van 31.3.2017, blz. 350.

Gedelegeerde Verordening (EU) 2017/571 van de Commissie	Gedelegeerde Verordening (EU) 2017/571 van de Commissie van 2 juni 2016 tot aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad met technische reguleringsnormen inzake vergunningverlening aan, organisatorische vereisten voor en publicatie van transactiemeldingen door aanbieders van datarapporteringsdiensten[17]
CSDR	Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012[18]
Gedelegeerde Verordening (EU) 2017/392 van de Commissie	Gedelegeerde Verordening (EU) 2017/392 van de Commissie van 11 november 2016 tot aanvulling van Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad met technische reguleringsnormen inzake de vergunnings-, toezichts- en operationele vereisten voor centrale effectenbewaarinstellingen[19]
RB-verordening	Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus[20]
Gedelegeerde Verordening (EU) nr. 449/2012 van de Commissie	Gedelegeerde Verordening (EU) nr. 449/2012 van de Commissie van 21 maart 2012 tot aanvulling van Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen betreffende te verstrekken gegevens voor de registratie en certificatie van ratingbureaus[21]
securitisatieverordening	Verordening (EU) 2017/2402 van het Europees Parlement en de Raad van 12 december 2017 tot vaststelling van een algemeen kader voor securitisatie en tot instelling van een specifiek kader voor eenvoudige, transparante en gestandaardiseerde securitisatie, en tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG en 2011/61/EU en de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 648/2012[22]
benchmarkverordening	Verordening (EU) 2016/1011 van het Europees Parlement en de Raad van 8 juni 2016 betreffende indices die worden gebruikt als benchmarks voor financiële instrumenten en

[17] PB L 87 van 31.3.2017, blz. 126.
[18] PB L 257 van 28.8.2014, blz. 1.
[19] PB L 65 van 10.3.2017, blz. 48.
[20] PB L 302 van 17.11.2009, blz. 1.
[21] PB L 140 van 30.5.2012, blz. 32.
[22] PB L 347 van 28.12.2017, blz. 35.

	financiële overeenkomsten of om de prestatie van beleggingsfondsen te meten en tot wijziging van Richtlijnen 2008/48/EG en 2014/17/EU en Verordening (EU) nr. 596/2014[23]
Gedelegeerde Verordening (EU) 2018/1646 van de Commissie	Gedelegeerde Verordening (EU) 2018/1646 van de Commissie van 13 juli 2018 tot aanvulling van Verordening (EU) 2016/1011 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen voor de informatie die moet worden verstrekt in een vergunningsaanvraag en een registratieaanvraag[24]
AVG	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[25]

Afkortingen

CSP	Aanbieder van clouddiensten (cloud service provider)
ESMA	Europese Autoriteit voor effecten en markten
EU	Europese Unie

Definities

functie	alle processen, diensten of activiteiten;
kritieke of belangrijke functie	een functie die bij een gebrekkige of tekortschietende uitvoering ervan wezenlijke nadelige gevolgen zou hebben voor: a) de naleving door een onderneming van haar verplichtingen uit hoofde van de toepasselijke wetgeving; b) de financiële prestaties van een onderneming; of c) de soliditeit of continuïteit van de belangrijkste diensten en activiteiten van een onderneming;
clouddiensten	diensten die worden geleverd met behulp van cloud computing;

[23] PB L 171 van 29.6.2016, blz. 1.
[24] PB L 274 van 5.11.2018, blz. 43.
[25] PB L 119 van 4.5.2016, blz. 1.

cloud computing of cloud[26]	een architectuur voor het verlenen van netwerktoegang tot een schaalbare en flexibele pool van deelbare fysieke of virtuele middelen (zoals servers, besturingssystemen, netwerken, software, applicaties en opslagmedia) met self-service levering en beheer op aanvraag;
aanbieder van clouddiensten	een derde die clouddiensten levert in het kader van een uitbestedingsovereenkomst betreffende clouddiensten;
uitbestedingsovereenkomst betreffende clouddiensten	een overeenkomst in welke vorm dan ook, inclusief delegatieregelingen, tussen: i) een onderneming en een CSP, waarbij deze CSP een functie verricht die anders door de onderneming zelf zou worden verricht; of ii) een onderneming en een derde die geen CSP is, maar die in belangrijke mate op een CSP beroep doet om een functie te verrichten die anders door de onderneming zelf zou worden verricht. In dit geval moet een verwijzing naar een “CSP” in deze richtsnoeren worden gelezen als een verwijzing naar deze derde;
onderuitbesteding	een situatie waarin de CSP op grond van een uitbestedingsovereenkomst de uitbestede functie (of een deel hiervan) verder overdraagt aan een andere dienstverlener;
cloud-implementatiemodel	de manier waarop de cloud kan worden ingericht op basis van het toezicht op en delen van fysieke of virtuele middelen. Cloud-implementatiemodellen zijn onder meer gemeenschappelijke[27], hybride[28], private[29] en publieke[30] clouds;
ondernemingen	a) beheerders van alternatieve beleggingsinstellingen of “abi-beheerders” zoals gedefinieerd in artikel 4, lid 1, onder b), van de AIFM-richtlijn en bewaarders als bedoeld in artikel 21, lid 3, van de AIFM-richtlijn (“bewaarders van

[26] Cloud computing wordt vaak afgekort tot “cloud”. In de rest van het document wordt gemakshalve de term “cloud” gebruikt.
[27] Een cloud-implementatiemodel waarbij clouddiensten uitsluitend ondersteuning bieden aan en worden gedeeld door een specifieke groep afnemers van clouddiensten die gedeelde behoeften en een onderlinge relatie hebben, en waarbij toezicht op de middelen wordt uitgeoefend door ten minste één lid van deze groep.
[28] Een cloud-implementatiemodel dat gebruikmaakt van ten minste twee verschillende modellen voor cloudimplementatie.
[29] Een cloud-implementatiemodel waarbij clouddiensten uitsluitend worden gebruikt door een enkele afnemer van clouddiensten en toezicht op de middelen wordt uitgeoefend door deze afnemer.
[30] Een cloud-implementatiemodel waarbij clouddiensten potentieel beschikbaar zijn voor elke afnemer van clouddiensten en toezicht op de middelen wordt uitgeoefend door de CSP.

alternatieve beleggingsinstellingen (abi's)");

b) beheermaatschappijen zoals gedefinieerd in artikel 2, lid 1, onder b), van de icbe-richtlijn ("icbe-beheermaatschappijen") en bewaarders zoals gedefinieerd in artikel 2, lid 1, onder a), van de icbe-richtlijn ("bewaarders van icbe's");

c) centrale tegenpartijen (CTP's) zoals gedefinieerd in artikel 2, lid 1, van EMIR en tier 2-CTP's uit derde landen in de zin van artikel 25, lid 2 bis, onder a), van EMIR die voldoen aan de relevante EMIR-voorschriften krachtens artikel 25, lid 2 ter, onder a), van EMIR;

d) transactieregisters zoals gedefinieerd in artikel 2, lid 2, van EMIR en in artikel 3, lid 1, van SFTR;

e) beleggingsondernemingen zoals gedefinieerd in artikel 4, lid 1, punt 1, van MiFID II en kredietinstellingen zoals gedefinieerd in artikel 4, lid 1, punt 27, van MiFID II die beleggingsdiensten en -activiteiten verrichten in de zin van artikel 4, lid 1, punt 2, van MiFID II;

f) aanbieders van datarapporteringsdiensten zoals gedefinieerd in artikel 4, lid 1, punt 63, van MiFID II[31];

g) marktexploitanten van handelsplatformen in de zin van artikel 4, lid 1, punt 24, van MiFID II;

h) centrale effectenbewaarinstellingen (central securities depositories – CSD's) zoals gedefinieerd in artikel 2, lid 1, punt 1, van de CSDR;

[31] Met ingang van 1 januari 2022 moet de verwijzing naar deze bepaling worden gelezen als verwijzing naar punt 36, onder a), van artikel 2, lid 1, van MiFIR.

i) ratingbureaus zoals gedefinieerd in artikel 3, lid 1, onder b), van de RB-verordening;

j) securitisatieregisters zoals gedefinieerd in artikel 2, lid 23, van de securitisatieverordening;

k) beheerders van cruciale benchmarks zoals gedefinieerd in artikel 3, lid 1, punt 25, van de benchmarkverordening.

III. Doel

5. Deze richtsnoeren zijn gebaseerd op artikel 16, lid 1, van de ESMA-verordening. Met deze richtsnoeren wordt beoogd consistente, doelmatige en doeltreffende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht (ESFS) vast te stellen en te zorgen voor de gemeenschappelijke, uniforme en consistente toepassing van de vereisten waarnaar wordt verwezen in paragraaf 1.1 onder het kopje “Wat?” wanneer ondernemingen activiteiten uitbesteden aan CSP’s. Deze richtsnoeren zijn met name bedoeld om ondernemingen en bevoegde autoriteiten te helpen de risico’s en uitdagingen van uitbestedingsovereenkomsten voor clouddiensten – van de beslissing tot uitbesteding, het selecteren van een CSP, het monitoren van uitbestede functies tot het ontwikkelen van exitstrategieën – in kaart te brengen, aan te pakken en te monitoren.

IV. Verplichtingen inzake naleving en rapportage

Status van de richtsnoeren

6. Volgens artikel 16, lid 3, van de ESMA-verordening moeten de bevoegde autoriteiten en ondernemingen zich tot het uiterste inspannen om aan deze richtsnoeren te voldoen.

7. Bevoegde autoriteiten waarvoor deze richtsnoeren gelden, leven deze na door ze voor zover van toepassing op te nemen in hun nationale wettelijke en/of toezichtkaders, ook wanneer bepaalde richtsnoeren in de eerste plaats gericht zijn op ondernemingen. In dit geval zorgen de bevoegde autoriteiten er door middel van hun toezicht voor dat ondernemingen de richtsnoeren naleven.

8. In het kader van haar doorlopende rechtstreekse toezicht zal ESMA de toepassing van deze richtsnoeren door ratingbureaus, TR’s, SR’s, tier 2-CTP’s uit derde landen en,

met ingang van 1 januari 2022, aanbieders van datarapporteringsdiensten en beheerders van voor de EU cruciale benchmarks beoordelen.

Rapportagevereisten

9. De bevoegde autoriteiten waarvoor deze richtsnoeren gelden, stellen ESMA er binnen twee maanden na de datum van bekendmaking van de richtsnoeren op de ESMA-website in alle officiële talen van de EU, van in kennis of zij i) voldoen, ii) niet voldoen, maar voornemens zijn te voldoen, of iii) niet voldoen en niet voornemens zijn te voldoen aan de richtsnoeren.

10. In geval van niet-naleving moeten de bevoegde autoriteiten ESMA ook binnen twee maanden na de datum van bekendmaking van de richtsnoeren op de website van ESMA in alle officiële talen van de EU in kennis stellen van de redenen waarom zij niet aan de richtsnoeren voldoen. Een formulier voor de kennisgevingen is beschikbaar op de website van ESMA. Zodra het formulier is ingevuld, wordt het aan ESMA toegezonden.

11. Ondernemingen zijn niet verplicht om te melden of zij aan deze richtsnoeren voldoen.

V. Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten

Richtsnoer 1. Governance, toezicht en documentatie

12. Een onderneming moet beschikken over een vastomlijnde en actuele uitbestedingsstrategie voor clouddiensten consistent met de relevante strategieën en interne beleidsmaatregelen en processen van de onderneming, waaronder met betrekking tot informatie- en communicatietechnologie, informatiebeveiliging en operationeel risicobeheer.

13. Een onderneming moet:

    a) de verantwoordelijkheden voor de documentatie en het beheer van en het toezicht op uitbestedingsovereenkomsten voor clouddiensten binnen haar organisatie duidelijk toekennen;
    b) voldoende middelen toewijzen om te waarborgen dat aan deze richtsnoeren en alle wettelijke vereisten die voor haar uitbestedingsovereenkomsten voor clouddiensten gelden wordt voldaan;
    c) een functie voor toezicht op de uitbesteding van clouddiensten in het leven roepen of senior medewerkers aanwijzen die rechtstreeks verantwoording afleggen aan het leidinggevend orgaan en verantwoordelijk zijn voor het beheer van en toezicht op de risico's van uitbestedingsovereenkomsten voor clouddiensten. Bij de naleving van dit richtsnoer moeten ondernemingen rekening houden met de aard, omvang en complexiteit van de onderliggende risico's, ook voor wat betreft het risico voor

het financiële systeem en de risico's die verbonden zijn aan de uitbestede functies, en ervoor zorgen dat hun leidinggevend orgaan over de benodigde technische vaardigheden beschikt om de risico's van uitbestedingsovereenkomsten voor clouddiensten te begrijpen[32]. Kleine en minder complexe ondernemingen moeten ten minste zorg dragen voor een duidelijke verdeling van taken en verantwoordelijkheden voor het management van en toezicht op uitbestedingsovereenkomsten voor clouddiensten.

14. Een onderneming moet de uitvoering van functies, de beveiligingsmaatregelen en de naleving van de overeengekomen niveaus van dienstverlening door haar aanbieders van clouddiensten monitoren. Deze monitoring moet risico gebaseerd zijn en vooral gericht zijn op kritieke of belangrijke uitbestede functies.

15. Een onderneming moet periodiek opnieuw beoordelen of haar uitbestedingsovereenkomsten voor clouddiensten een kritieke of belangrijke functie betreffen, en eveneens een dergelijke beoordeling verrichten wanneer een wezenlijke wijziging voordoet in het risico, de aard of de omvang van de uitbestede functie.

16. Een onderneming moet een geactualiseerd register bijhouden met informatie over al haar uitbestedingsovereenkomsten voor clouddiensten en daarbij onderscheid maken tussen de uitbesteding van kritieke of belangrijke functies en niet als kritiek of belangrijk aangemerkte functies. Hierbij moet zij kort aangeven waarom de uitbestede functie al dan niet kritiek of belangrijk wordt geacht. Met inachtneming van het nationaal recht moet een onderneming daarnaast gedurende een passende periode een lijst van beëindigde uitbestedingsovereenkomsten voor clouddiensten bijhouden.

17. Voor de uitbestedingsovereenkomsten voor clouddiensten voor kritieke of belangrijke functies moet het register voor elke uitbestedingsovereenkomst voor clouddiensten ten minste de volgende informatie bevatten:

    a) een referentienummer;
    b) de aanvangsdatum en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, de einddatum en/of opzeggingstermijnen voor de CSP en voor de onderneming;
    c) een korte beschrijving van de uitbestede functie, met inbegrip van de uitbestede gegevens en de vermelding of deze gegevens persoonsgegevens omvatten (bijvoorbeeld door in een afzonderlijk gegevensveld Ja of Nee in te vullen);
    d) een door de onderneming toegewezen categorie die de aard van de uitbestede functie aangeeft (bijvoorbeeld IT-functie, toezichtfunctie), die het gemakkelijker moet maken om de verschillende soorten uitbestedingsovereenkomsten voor clouddiensten te identificeren;
    e) vermelding of de uitbestede functie ter ondersteuning dient van tijdgevoelige bedrijfsactiviteiten;

[32] Zie de gemeenschappelijke ESMA- en EBA-richtsnoeren voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie uit hoofde van Richtlijn 2013/36/EU en Richtlijn 2014/65/EU voor beleggingsondernemingen en kredietinstellingen (EBA/GL/2017/12).

f) de naam en de merknaam (indien van toepassing) van de CSP, het land waar deze is geregistreerd, het handelsregisternummer, de identificatiecode voor rechtspersonen (indien van toepassing), het geregistreerde adres, de relevante contactgegevens en de naam van de moederonderneming van het bedrijf (indien van toepassing);
g) het toepasselijke recht waardoor de uitbestedingsovereenkomst voor clouddiensten wordt beheerst, en, indien van toepassing, de jurisdictiekeuze;
h) het soort clouddiensten en implementatiemodellen en de specifieke aard van de te bewaren gegevens alsook de locaties (te weten landen of regio's) waar die gegevens kunnen worden opgeslagen;
i) de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst is beoordeeld en de datum van de volgende geplande beoordeling;
j) de datum van de meest recente risicobeoordeling/audit van de CSP alsmede een korte samenvatting van de belangrijkste resultaten, en de datum van de volgende geplande risicobeoordeling/audit;
k) de persoon of het besluitvormingsorgaan binnen de onderneming die/dat de uitbestedingsovereenkomst betreffende clouddiensten heeft goedgekeurd;
l) indien van toepassing, de namen van onderaannemers waaraan kritieke of belangrijke onderdelen (of wezenlijke onderdelen daarvan) zijn onderuitbesteed, inclusief de landen waar de onderaannemers zijn geregistreerd, waar de onderuitbestede dienst zal worden verricht en de locatie (te weten landen of regio's) waar de gegevens zullen worden opgeslagen;
m) de geraamde jaarlijkse begrotingskosten van de uitbestedingsovereenkomst voor clouddiensten.

18. Voor de uitbestedingsovereenkomsten voor clouddiensten voor niet-kritieke of niet-belangrijke functies moet een onderneming op basis van de aard, de omvang en complexiteit van de aan de uitbestede functie verbonden risico's bepalen welke gegevens in het register worden opgenomen.

Richtsnoer 2. Analyse voorafgaand aan uitbesteding en due diligence

19. Voordat een onderneming een uitbestedingsovereenkomst voor clouddiensten aangaat, moet zij:

a) beoordelen of de uitbestedingsovereenkomst voor clouddiensten betrekking heeft op een kritieke of belangrijke functie;
b) alle relevante risico's van de uitbestedingsovereenkomst betreffende clouddiensten vaststellen en beoordelen;
c) een passend due diligence-onderzoek uitvoeren ten aanzien van de potentiële CSP;
d) mogelijke belangenconflicten als gevolg van de uitbesteding identificeren en beoordelen.

20. De voorafgaand aan uitbesteding verrichte analyse en het due diligence-onderzoek ten aanzien van de potentiële CSP moeten in verhouding staan tot de aard, de omvang en

complexiteit van de functie die de onderneming wil uitbesteden en de risico's die met deze functie verbonden zijn. Er moet in elk geval een beoordeling worden uitgevoerd van de mogelijke gevolgen van de uitbestedingsovereenkomst voor clouddiensten voor de operationele, juridische, nalevings- en reputatierisico's voor de onderneming.

21. Ingeval de uitbestedingsovereenkomst voor clouddiensten kritieke of belangrijke functies betreft, moet een onderneming ook:

    a) een beoordeling maken van alle relevante risico's die kunnen voortvloeien uit de uitbestedingsovereenkomst voor clouddiensten, waaronder risico's met betrekking tot informatie- en communicatietechnologie, informatiebeveiliging, bedrijfscontinuïteit, juridische, nalevings-, reputatie- en operationele risico's, alsmede mogelijke toezichtsbelemmeringen voor de onderneming die het gevolg zijn van:
        i. de geselecteerde clouddienst en de voorgestelde implementatiemodellen;
        ii. het migratie- en/of uitvoeringsproces;
        iii. de gevoeligheid van de functie en de betrokken gegevens die het bedrijf eventueel wil uitbesteden en de beveiligingsmaatregelen die zouden moeten worden genomen;
        iv. de interoperabiliteit van de systemen en applicaties van de onderneming en van de CSP, dat wil zeggen hun vermogen om informatie uit te wisselen en deze uitgewisselde informatie te gebruiken;
        v. de overdraagbaarheid van de gegevens van de onderneming, te weten de mogelijkheid om de ondernemingsgegevens eenvoudig van de ene CSP over te dragen aan een andere aanbieder of aan de onderneming zelf;
        vi. de politieke stabiliteit, de veiligheidssituatie en het rechtssysteem (met inbegrip van de geldende rechtshandhavingsbepalingen, de bepalingen uit het insolventierecht die van toepassing zouden zijn in geval van faillissement van de CSP, de geldende regelgeving inzake gegevensbescherming en de vraag of er is voldaan aan de voorwaarden voor de overdracht van persoonsgegevens aan een derde land overeenkomstig de AVG) van de landen (binnen of buiten de EU) waar de uitbestede functies zouden worden verricht en waar de uitbestede gegevens zouden worden opgeslagen; in het geval van onderuitbesteding, de aanvullende risico's die kunnen ontstaan als de onderaannemer zich in een derde land of in een ander land dan de CSP bevindt en, in het geval van een onderuitbestedingsketen, elk aanvullend risico dat zich kan voordoen, ook door het ontbreken van een directe overeenkomst tussen de onderneming en de onderaannemer die de uitbestede functie verricht;
        vii. een mogelijke concentratie binnen de onderneming (waar van toepassing tevens op het niveau van de groep waarvan de onderneming deel uitmaakt) die wordt veroorzaakt doordat met één en dezelfde CSP meerdere uitbestedingsovereenkomsten voor clouddiensten zijn aangegaan, en een mogelijke concentratie binnen de financiële sector in de EU doordat meerdere ondernemingen gebruikmaken van dezelfde CSP of een kleine groep van aanbieders van clouddiensten. Bij de beoordeling van het concentratierisico moet de onderneming al haar

uitbestedingsovereenkomsten voor clouddiensten met die CSP in aanmerking nemen (en, waar van toepassing, de uitbestedingsovereenkomsten voor clouddiensten op het niveau van de groep waarvan zij deel uitmaakt);

b) rekening houden met de verwachte voordelen en kosten van de uitbestedingsovereenkomst betreffende clouddiensten, met inbegrip van een afweging tussen de significante risico's die kunnen worden verkleind of beter kunnen worden beheerd, en eventuele significante risico's die zich kunnen voordoen als gevolg van de uitbestedingsovereenkomst betreffende clouddiensten.

22. In geval van uitbesteding van kritieke of belangrijke functies moet een evaluatie van de geschiktheid van de CSP deel uitmaken van het due diligence-onderzoek. Bij de beoordeling van de geschiktheid van de CSP moet een onderneming ervoor zorgen dat de CSP over de bedrijfsreputatie, de vaardigheden, de middelen (waaronder personele, IT- en financiële middelen), de organisatiestructuur en, indien van toepassing, de benodigde vergunning(en) of registratie(s) beschikt om de kritieke of belangrijke functie op betrouwbare en professionele wijze te verrichten en zijn verplichtingen gedurende de looptijd van de uitbestedingsovereenkomst voor clouddiensten na te komen. Aanvullende factoren die in een due diligence-onderzoek naar de CSP moeten worden onderzocht, zijn onder meer:

    a) het beheer van informatiebeveiliging en met name de bescherming van persoonsgegevens en vertrouwelijke of anderszins gevoelige gegevens;
    b) de door de CSP geboden support, met inbegrip van supportplannen en contactpersonen voor support, en procedures op het gebied van incidentenbeheer;
    c) de plannen inzake bedrijfscontinuïteit en rampenherstel.

23. Waar van toepassing en om het uitgevoerde due diligence-onderzoek te ondersteunen, kan een onderneming tevens gebruikmaken van certificeringen op basis van internationale normen en verslagen van externe of interne audits.

24. Als een onderneming aanzienlijke tekortkomingen en/of veranderingen in de verrichte diensten of de situatie van de CSP vaststelt, moeten de voorafgaand aan uitbesteding verrichte analyse en het due diligence-onderzoek ten aanzien van de aanbieder onmiddellijk worden herzien of waar nodig opnieuw worden uitgevoerd.

25. Indien een onderneming een nieuwe overeenkomst sluit met een reeds beoordeelde CSP of een bestaande overeenkomst verlengt, moet zij middels een op risico gebaseerde benadering vaststellen of er een nieuw due diligence-onderzoek nodig is.

Richtsnoer 3. Essentiële contractuele bepalingen

26. De respectievelijke rechten en plichten van een onderneming en haar CSP moeten duidelijk in een schriftelijke overeenkomst worden vastgelegd.

27. De schriftelijke overeenkomst moet de onderneming uitdrukkelijk de mogelijkheid bieden om de overeenkomst indien nodig te beëindigen.

28. In geval van uitbesteding van kritieke of belangrijke functies moet de schriftelijke overeenkomst minimaal het volgende bevatten:

a) een heldere beschrijving van de uitbestede functie;

b) de aanvangsdatum en de einddatum van de overeenkomst, indien van toepassing, en de opzegtermijnen voor de CSP en de onderneming;

c) het toepasselijke recht dat op de overeenkomst van toepassing is, en, indien van toepassing, de jurisdictiekeuze;

d) de financiële verplichtingen van de onderneming en van de CSP;

e) vermelding of onderuitbesteding is toegestaan en zo ja, onder welke voorwaarden, gelet op richtsnoer 7;

f) de locatie(s) (te weten landen of regio's) waar de uitbestede functie zal worden verricht en gegevens zullen worden verwerkt en opgeslagen, en de voorwaarden waaraan moet worden voldaan, met inbegrip van een verplichting om de onderneming in kennis te stellen als de CSP voorstelt de locatie(s) te wijzigen;

g) de bepalingen inzake informatiebeveiliging en de bescherming van persoonsgegevens, gelet op richtsnoer 4;

h) het recht voor de onderneming om de prestaties van de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten regelmatig te monitoren, gelet op richtsnoer 6;

i) de overeengekomen niveaus van dienstverlening, die kwantitatieve en kwalitatieve prestatiedoelen moeten omvatten om tijdige controle mogelijk te maken, zodat zonder onnodig uitstel passende corrigerende beheersmaatregelen kunnen worden genomen indien de overeengekomen dienstverleningsniveaus niet worden gehaald;

j) de verplichtingen van de CSP tot verslaglegging aan de onderneming, en, indien nodig, de verplichtingen om verslagen in te dienen die relevant zijn voor de veiligheidsfunctie en cruciale functies van de onderneming, zoals verslagen van de interne-auditfunctie van de CSP;

k) de bepalingen inzake het incidentenbeheer door de CSP, met inbegrip van de verplichting voor de CSP om de onderneming zonder onnodig uitstel op de hoogte te stellen van incidenten die de uitvoering van de uitbestede dienst van de onderneming hebben beïnvloed;

l) vermelding of de CSP zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking;

m) de verplichting van de CSP om de plannen voor bedrijfscontinuïteit en rampenherstel in te voeren en te testen;

n) de verplichting van de CSP om de onderneming, de betreffende bevoegde autoriteiten en elke andere door de onderneming of de bevoegde autoriteiten aangewezen persoon toegangsrechten en voor de relevante informatie, locaties, systemen en apparaten van de CSP inspectierechten (onderzoeks- en

"auditrechten") toe te kennen voor zover deze nodig zijn om de prestaties van de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten en zijn naleving van de geldende wettelijke voorschriften en contractuele vereisten te monitoren, gelet op richtsnoer 6;

o) bepalingen om te waarborgen dat de gegevens die de CSP namens de onderneming verwerkt of opslaat, waar nodig toegankelijk zijn en kunnen worden hersteld en geretourneerd aan de onderneming, gelet op richtsnoer 5.

Richtsnoer 4. Informatiebeveiliging

29. Een onderneming moet informatiebeveiligingseisen opnemen in haar interne beleid en procedures en in de schriftelijke uitbestedingsovereenkomst voor clouddiensten en de naleving van deze eisen voortdurend monitoren, mede om vertrouwelijke, persoons- of anderszins gevoelige gegevens te beschermen. Deze eisen moeten in verhouding staan tot de aard, schaal en complexiteit van de functie die de onderneming uitbesteedt aan de CSP en de risico's die met deze functie verbonden zijn.

30. Daarvoor moet een onderneming in geval van uitbesteding van kritieke of belangrijke functies, en zonder afbreuk te doen aan de toepasselijke eisen uit de AVG, middels een op risico gebaseerde benadering ten minste:

a) *organisatie voor informatiebeveiliging:* waarborgen dat informatiebeveiligingsrollen en -verantwoordelijkheden duidelijk zijn verdeeld tussen de onderneming en de CSP, ook met betrekking tot detectie van bedreigingen, incidenten- en patchbeheer, en dat de CSP zijn rollen en verantwoordelijkheden daadwerkelijk kan vervullen en na kan komen;
b) *identiteits- en toegangsbeheer*: ervoor zorgen dat er sterke authenticatiemechanismen (bijvoorbeeld tweefactorauthenticatie) en toegangsmaatregelen zijn geïmplementeerd om ongeoorloofde toegang tot de gegevens en back-end cloudresources van de onderneming te voorkomen;
c) *versleuteling en sleutelbeheer:* ervoor zorgen dat er waar nodig gebruik wordt gemaakt van relevante versleutelingstechnologieën voor gegevens in transit, opgeslagen gegevens, gegevens in rusttoestand en gegevensback-ups in combinatie met passende sleutelbeheeroplossingen om het risico van ongeoorloofde toegang tot versleutelingscodes te beperken; met name bij de keuze van een sleutelbeheeroplossing moet de onderneming aandacht besteden aan geavanceerde technologie en processen ;
d) *operationele en netwerkbeveiliging:* aandacht besteden aan passende niveaus van beschikbaarheid en scheiding van netwerken (bijvoorbeeld tenantisolatie in de gedeelde cloudomgeving, operationele scheiding van web, applicatielogica, besturingssysteem, netwerk, database management systeem (DBMS) en opslaglagen) en verwerkingsomgevingen (bijvoorbeeld test-, gebruikersacceptatietest-, ontwikkel- en productieomgeving);
e) *application programming interfaces (API's):* aandacht besteden aan mechanismen voor de integratie van de clouddiensten met de systemen van de onderneming om de veiligheid van API's te waarborgen (bijvoorbeeld door voor meerdere

systeeminterfaces, jurisdicties en bedrijfsfuncties informatiebeveiligingsbeleid en -procedures voor API's op te zetten en te onderhouden om ongeoorloofde openbaarmaking, wijziging of vernietiging van gegevens te voorkomen);

f) *bedrijfscontinuïteit en rampenherstel*: zorgen voor doeltreffende beheersmaatregelen ten aanzien van bedrijfscontinuïteit en rampenherstel (bijvoorbeeld door minimumcapaciteitsvereisten vast te stellen, geografisch gespreide hostingopties te selecteren waarbij tussen de verschillende opties kan worden gewisseld, of door documentatie op te vragen en door te nemen die laat zien welke route de gegevens van de onderneming tussen de systemen van de CSP volgen, alsmede door de mogelijkheid te overwegen om machine images naar een onafhankelijke opslaglocatie te kopiëren die voldoende geïsoleerd is van het netwerk of offline is);

g) *gegevenslocatie*: een op risico gebaseerde benadering volgen ten aanzien van gegevensopslag- en gegevensverwerkingslocatie(s) (te weten landen of regio's);

h) *naleving en monitoring*: verifiëren dat de CSP voldoet aan internationaal erkende informatiebeveiligingsnormen en passende informatiebeveiligingsmaatregelen heeft geïmplementeerd (bijvoorbeeld door de CSP te vragen aan te tonen dat hij relevante informatiebeveiligingsmaatregelen uitvoert en de informatiebeveiligingsmaatregelen van de CSP regelmatig beoordeelt en test).

Richtsnoer 5. Exitstrategieën

31. In geval van uitbesteding van kritieke of belangrijke functies moet een onderneming ervoor zorgen dat zij de uitbestedingsovereenkomst voor clouddiensten kan beëindigen zonder onnodige verstoring van haar bedrijfsactiviteiten en dienstverlening aan klanten en zonder dat de naleving van haar verplichtingen uit hoofde van de toepasselijke wetgeving en de vertrouwelijkheid, integriteit en beschikbaarheid van haar gegevens enig nadeel ondervinden. Daarvoor moet een onderneming:

    a) exitplannen ontwikkelen en implementeren die volledig, gedocumenteerd en voldoende getest zijn. Deze plannen moeten waar nodig worden geactualiseerd, onder meer in geval van wijzigingen in de uitbestede functie;

    b) met alternatieve oplossingen komen en overgangsplannen ontwikkelen om de uitbestede functie en gegevens bij de CSP en, indien van toepassing, bij eventuele onderaannemers weg te halen en over te dragen aan de andere CSP, zoals aangegeven door de onderneming, of rechtstreeks aan de onderneming zelf. Deze oplossingen moeten worden vastgesteld met het oog op de uitdagingen die zich kunnen voordoen door de locatie van de gegevens, en daarbij moeten de nodige beheersmaatregelen worden genomen om de bedrijfscontinuïteit tijdens de overgangsfase te waarborgen;

    c) ervoor zorgen dat de schriftelijke uitbestedingsovereenkomst voor de CSP de verplichting omvat om de uitbestede functie en de daarmee samenhangende verwerking van gegevens ordentelijk over te dragen van de CSP en eventuele onderaannemers aan een andere CSP, zoals aangegeven door de onderneming, of rechtstreeks aan de onderneming zelf ingeval de onderneming de exitstrategie in werking stelt. De verplichting om de ordentelijke overdracht van de uitbestede functie en de daarmee samenhangende verwerking van gegevens te

ondersteunen moet waar relevant ook de veilige verwijdering van de gegevens uit de systemen van de CSP en eventuele onderaannemers omvatten.

32. Bij de ontwikkeling van de exitplannen en oplossingen waarnaar wordt verwezen in de bovenstaande punten a) en b) (“exitstrategie”) moet de onderneming aandacht besteden aan:

    a) de vaststelling van de doelen van de exitstrategie;
    b) de aanwijzing van gebeurtenissen waarbij de exitstrategie in werking kan worden gesteld. Hiertoe moeten in elk geval de beëindiging van de uitbestedingsovereenkomst voor clouddiensten op initiatief van de onderneming of de CSP en het faillissement of een andere ernstige onderbreking van de bedrijfsactiviteiten van de CSP worden gerekend;
    c) de uitvoering van een effectbeoordeling van de potentiële bedrijfsschade die in verhouding staat tot de uitbestede functie om na te gaan welke personele en andere middelen er nodig zouden zijn om de exitstrategie uit te voeren;
    d) de toewijzing van rollen en verantwoordelijkheden voor het beheer van de exitstrategie;
    e) de toetsing van de geschiktheid van de exitstrategie te testen middels een op risico gebaseerde benadering (bijvoorbeeld door middel van een analyse van de potentiële kosten, gevolgen, middelen en implicaties voor de tijdsplanning van de overdracht van een uitbestede dienst aan een andere aanbieder);
    f) de opstelling van criteria om te bepalen of de overgang is geslaagd.

33. Een onderneming moet indicatoren van de gebeurtenissen waarbij de exitstrategie in werking kan worden gesteld opnemen in haar doorlopende monitoring van en toezicht op de diensten die de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten verricht.

Richtsnoer 6. Toegangs- en auditrecht

34. Een onderneming moet ervoor zorgen dat de schriftelijke uitbestedingsovereenkomst voor clouddiensten geen beperkingen oplegt aan de doeltreffende uitoefening van het toegangs- en auditrecht en toezichtopties ten aanzien van de CSP door de onderneming en de bevoegde autoriteit.

35. Een onderneming moet ervoor zorgen dat bij de uitoefening van het toegangs- en auditrecht (zoals de auditfrequentie en de te controleren gebieden en diensten) rekening wordt gehouden met de vraag of de uitbesteding verband houdt met een kritieke of belangrijke functie en met de aard en omvang van de risico’s en gevolgen van de uitbestedingsovereenkomst voor clouddiensten voor de onderneming.

36. Ingeval de uitoefening van het toegangs- of auditrecht of het gebruik van bepaalde audittechnieken een risico oplevert voor de omgeving van de CSP en/of een andere klant van de CSP (bijvoorbeeld doordat deze/dit gevolgen heeft voor de dienstverleningsniveaus of de vertrouwelijkheid, integriteit en beschikbaarheid van

gegevens), moet de CSP duidelijk aangeven waarom dit een risico zou opleveren en samen met de onderneming alternatieve werkwijzen overeenkomen om een vergelijkbaar resultaat te bereiken (bijvoorbeeld de opname van specifieke beheersmaatregelen die worden getest in een specifiek verslag/specifieke certificering van de CSP).

37. Onverminderd hun eindverantwoordelijkheid ten aanzien van uitbestedingsovereenkomsten voor clouddiensten kunnen ondernemingen, om hun auditmiddelen efficiënter aan te wenden en de organisatorische lasten voor de CSP en zijn klanten te verlichten, gebruikmaken van:

    a) door de CSP verstrekte externe certificeringen en externe of interne auditrapportages;
    b) gemeenschappelijke audits die samen met andere klanten van dezelfde CSP of door een door meerdere klanten van dezelfde CSP aangestelde externe auditor worden uitgevoerd.

38. In geval van uitbesteding van kritieke of belangrijke functies moet een onderneming beoordelen of de in punt 37, onder a), bedoelde externe certificeringen en externe of interne auditverslagen passend en toereikend zijn om aan haar verplichtingen uit hoofde van de toepasselijke wetgeving te voldoen, en moet zij ernaar streven na verloop van tijd niet uitsluitend gebruik te maken van deze certificeringen en verslagen.

39. In geval van uitbesteding van kritieke of belangrijke functies mag een onderneming alleen gebruikmaken van de in punt 37, onder a), bedoelde externe certificeringen en externe of interne auditverslagen als zij:

    a) erop toeziet dat de certificeringen of auditverslagen betrekking hebben op de essentiële systemen van de CSP (bijvoorbeeld processen, applicaties, infrastructuur, gegevenscentra), de door de onderneming vastgestelde essentiële beheersmaatregelen en de naleving van de relevante toepasselijke wetgeving;
    b) de inhoud van de certificeringen of auditverslagen regelmatig grondig beoordeelt en nagaat of de certificeringen of verslagen niet verouderd zijn;
    c) erop toeziet dat ook toekomstige versies van de certificeringen of auditverslagen betrekking hebben op essentiële systemen en beheersmaatregelen van de CSP;
    d) zich heeft vergewist van de geschiktheid van de certificerende of controlerende partij (bijvoorbeeld met betrekking tot de kwalificaties, deskundigheid, herhaling van de uitvoering/controle van bewijsstukken in het betrokken auditdossier en de roulering van de certificerende of controlerende organisatie);
    e) zich ervan heeft vergewist dat de certificeringen zijn afgegeven, dat de audits zijn uitgevoerd overeenkomstig passende normen en dat deze een toetsing omvatten van de doeltreffendheid van de aanwezige essentiële beheersmaatregelen;
    f) contractueel gerechtigd is te verzoeken om uitbreiding van de reikwijdte van de certificeringen of auditverslagen tot andere relevante systemen en beheersmaatregelen van de CSP, waarbij geldt dat het aantal en de frequentie van dergelijke verzoeken redelijk en vanuit het oogpunt van risicobeheer gerechtvaardigd moeten zijn;

g) het contractuele recht behoudt om naar eigen inzicht individuele audits op locatie uit te voeren ten aanzien van de uitbestede functie.

40. Een onderneming moet de CSP voorafgaand aan een locatiebezoek – ook van een derde door de onderneming aangewezen partij (bijvoorbeeld een auditor) – hiervan binnen een redelijke termijn vooraf in kennis stellen, tenzij een voorafgaande kennisgeving niet mogelijk is vanwege een noodgeval of crisissituatie of tot een situatie zou leiden waarin de audit niet langer doeltreffend zou zijn. In deze kennisgeving moeten de locatie en het doel van het bezoek worden vermeld, evenals het personeel dat aan het bezoek zal deelnemen.

41. Aangezien clouddiensten technisch bijzonder complex zijn en specifieke uitdagingen op het gebied van bevoegdheid met zich meebrengen, moet het personeel dat de audit verricht – de interne auditors van de onderneming of de namens haar handelende auditors – over de juiste vaardigheden en kennis beschikken om de betreffende clouddiensten te beoordelen en een doeltreffende en relevante audit te verrichten. Hetzelfde moet gelden voor het personeel van de onderneming dat de certificeringen of auditverslagen van de CSP evalueert.

Richtsnoer 7. Onderuitbesteding

42. Indien onderuitbesteding van kritieke of belangrijke functies (of wezenlijke onderdelen daarvan) is toegestaan, moet(en) in de schriftelijke uitbestedingsovereenkomst voor clouddiensten tussen de onderneming en de CSP:

a) elk deel of aspect van de uitbestede functie worden aangegeven dat van potentiële onderuitbesteding is uitgesloten;
b) de voorwaarden worden vermeld waaraan in het geval van onderuitbesteding moet worden voldaan.
c) worden aangegeven dat de CSP aansprakelijk blijft en de onderuitbestede diensten moet monitoren en controleren, om te waarborgen dat alle contractuele verplichtingen tussen hem en de onderneming voortdurend worden nagekomen;
d) een verplichting worden opgenomen voor de CSP om de onderneming in kennis te stellen van elke beoogde onderuitbesteding of wezenlijke wijzigingen daarvan, met name waar deze gevolgen kan hebben voor het vermogen van de CSP om aan zijn verplichtingen uit hoofde van de uitbestedingsovereenkomst voor clouddiensten met de onderneming te voldoen. De in de schriftelijke overeenkomst vastgelegde kennisgevingstermijn moet de onderneming voldoende tijd bieden om ten minste een risicobeoordeling van de voorgestelde onderuitbesteding of wezenlijke wijzigingen daarvan uit te voeren en hiertegen bezwaar te maken dan wel deze uitdrukkelijk goed te keuren, zoals hieronder aangegeven in punt e);
e) worden gewaarborgd dat de onderneming het recht heeft bezwaar te maken tegen de beoogde onderuitbesteding of wezenlijke wijzigingen daarvan, of dat expliciete

goedkeuring nodig is voordat de voorgestelde onderuitbesteding of wezenlijke wijzigingen van kracht worden;

f) worden gewaarborgd dat de onderneming contractueel gerechtigd is de uitbestedingsovereenkomst voor clouddiensten met de CSP te beëindigen ingeval zij bezwaar maakt tegen de voorgestelde onderuitbesteding of wezenlijke wijzigingen daarvan en in geval van onrechtmatige onderuitbesteding (bijvoorbeeld wanneer de CSP overgaat tot onderuitbesteding zonder de onderneming hiervan in kennis te stellen of de voorwaarden van de onderuitbesteding zoals vermeld in de uitbestedingsovereenkomst ernstig schendt).

43. De onderneming dient ervoor te zorgen dat de CSP adequaat toezicht houdt over de onderaannemer.

Richtsnoer 8. Schriftelijke kennisgeving aan bevoegde autoriteiten

44. De onderneming moet de bevoegde autoriteit tijdig schriftelijk in kennis stellen van geplande uitbestedingsovereenkomsten voor clouddiensten die een kritieke of belangrijke functie betreffen. Daarnaast moet de onderneming de bevoegde autoriteit tijdig schriftelijk in kennis stellen van die uitbestedingsovereenkomsten voor clouddiensten die een functie betreffen die eerder als niet-kritiek of niet-belangrijk werd aangemerkt en vervolgens kritiek of belangrijk werd.

45. De schriftelijke kennisgeving van de onderneming moet, met inachtneming van het evenredigheidsbeginsel, ten minste de volgende informatie bevatten:

a) de aanvangsdatum van de uitbestedingsovereenkomst voor clouddiensten en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, en de einddatum en/of opzeggingstermijnen voor de CSP en voor de onderneming;
b) een korte beschrijving van de uitbestede functie;
c) een korte samenvatting van de redenen waarom de uitbestede functie kritiek of belangrijk wordt geacht;
d) de naam en de merknaam (indien van toepassing) van de CSP, het land waar deze is geregistreerd, het handelsregisternummer, de identificatiecode voor rechtspersonen (indien van toepassing), het geregistreerde adres, de relevante contactgegevens en de naam van de moederonderneming van het bedrijf (indien van toepassing);
e) het toepasselijke recht waardoor de uitbestedingsovereenkomst voor clouddiensten wordt beheerst, en, indien van toepassing, de jurisdictiekeuze;
f) de implementatiemodellen voor clouddiensten en de specifieke aard van de door de CSP te bewaren gegevens en de locaties (te weten landen of regio's) waar die gegevens zullen worden opgeslagen;
g) de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst is beoordeeld;
h) de datum van de meest recente risicobeoordeling of audit van de CSP alsmede een korte samenvatting van de belangrijkste resultaten, en de datum van de volgende geplande risicobeoordeling of audit;

i) de persoon of het besluitvormingsorgaan binnen de onderneming die/dat de uitbestedingsovereenkomst betreffende clouddiensten heeft goedgekeurd;
j) indien van toepassing, de namen van de onderaannemer waaraan wezenlijke onderdelen van een kritieke of belangrijke functie zijn onderuitbesteed, inclusief het land of de regio waar de onderaannemers zijn geregistreerd, waar de onderuitbestede dienst zal worden verricht en waar de gegevens zullen worden opgeslagen.

Richtsnoer 9. Toezicht op uitbestedingsovereenkomsten voor clouddiensten

46. Als onderdeel van hun toezichtproces moeten bevoegde autoriteiten de risico's die voortvloeien uit door de onderneming gesloten uitbestedingsovereenkomsten betreffende clouddiensten beoordelen. Deze beoordeling moet vooral zijn gericht op de overeenkomsten die betrekking hebben op de uitbesteding van kritieke of belangrijke functies.

47. Bevoegde autoriteiten vergewissen zich ervan dat zij doeltreffend toezicht kunnen uitoefenen, vooral wanneer ondernemingen kritieke of belangrijke functies uitbesteden die buiten de EU worden verricht.

48. Bevoegde autoriteiten moeten op basis van een risicogebaseerde aanpak beoordelen of ondernemingen:

a) beschikken over de nodige governance, middelen en operationele processen om waar nodig en doeltreffend uitbestedingsovereenkomsten betreffende clouddiensten te sluiten, uit te voeren en hierop toezicht te houden;
b) alle relevante risico's in verband met de uitbesteding betreffende clouddiensten identificeren en beheren.

49. Wanneer concentratierisico's worden vastgesteld, moeten bevoegde autoriteiten de ontwikkeling van deze risico's monitoren en de mogelijke gevolgen hiervan voor andere ondernemingen waarop zij toezicht uitoefenen en voor de stabiliteit van de financiële markt evalueren.