EIOPA-BoS-20-002

Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten

Inhoudsopgave

Inleiding

1. Overeenkomstig artikel 16 van Verordening (EU) nr. 1094/2010[1] vaardigt Eiopa richtsnoeren uit om verzekerings- en herverzekeringsondernemingen te helpen met de toepassing van de uitbestedingsbepalingen van Richtlijn 2009/138/EG[2] ("richtlijn Solvabiliteit II") en Gedelegeerde Verordening (EU) 2015/35 van de Commissie[3] ("gedelegeerde verordening") in het geval van uitbesteding aan aanbieders van clouddiensten

2. Deze richtsnoeren zijn gebaseerd op artikel 13, punt 28, en de artikelen 38 en 49 van de richtlijn Solvabiliteit II en artikel 274 van de gedelegeerde verordening. Verder bouwen deze richtsnoeren voort op de Eiopa-richtsnoeren voor het governancesysteem (Eiopa-BoS-14/253).

3. Deze richtsnoeren zijn bedoeld voor bevoegde autoriteiten en dienen als leidraad voor verzekerings- en herverzekeringsondernemingen (hierna: "onderneming(en)" bij de toepassing van de uitbestedingsvoorschriften uit de bovengenoemde richtlijn en verordening in het kader van uitbesteding aan aanbieders van clouddiensten.

4. De richtsnoeren gelden voor individuele ondernemingen en mutatis mutandis ook voor groepen[4].

   De entiteiten waarvoor andere sectorale voorschriften gelden en die deel uitmaken van een groep, vallen op individueel niveau buiten het toepassingsgebied van deze richtsnoeren, aangezien zij zich zowel aan de specifieke sectorale voorschriften als aan de relevante richtsnoeren van de Europese Autoriteit voor effecten en markten en de Europese Bankautoriteit moeten houden.

5. In het geval van uitbesteding binnen de groep en onderuitbesteding aan aanbieders van clouddiensten moeten deze richtsnoeren worden toegepast in samenhang met de bepalingen van de Eiopa-richtsnoeren voor het governancesysteem over uitbesteding binnen een groep.

6. Bij de naleving van deze richtsnoeren of het toezicht daarop moeten ondernemingen en bevoegde autoriteiten rekening houden met het evenredigheidsbeginsel[5] en de mate waarin de aan aanbieders van clouddiensten uitbestede dienst kritiek of belangrijk is. Het evenredigheidsbeginsel moet ervoor zorgen dat governanceregelingen, met inbegrip van de met aanbieders van clouddiensten gesloten uitbestedingsovereenkomsten, in verhouding staan tot de aard, de omvang en de complexiteit van de onderliggende risico's.

7. Deze richtsnoeren moeten in samenhang met en onverminderd de Eiopa-richtsnoeren voor het governancesysteem en de vereisten uit punt 1 daarvan worden gelezen.

---

[1] 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).

[2] Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1).

[3] Gedelegeerde Verordening (EU) 2015/35 van de Commissie van 10 oktober 2014 tot aanvulling van Richtlijn 2009/138/EG van het Europees Parlement en de Raad betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 12 van 17.1.2015, blz. 1).

[4] Artikel 212, lid 1, van de richtlijn Solvabiliteit II.

[5] Artikel 29, lid 3, van de richtlijn Solvabiliteit II.

Definities

8. Termen die niet zijn gedefinieerd in deze richtsnoeren, hebben de betekenis die is vastgelegd in de richtlijn en de verordening waarnaar in de inleiding is verwezen.

9. In deze richtsnoeren gelden daarnaast de volgende definities:

Dienstverlener:	een derde die een proces, dienst of activiteit, of onderdelen daarvan, verleent of uitvoert op grond van een uitbestedingsovereenkomst.
Aanbieder van clouddiensten:	een dienstverlener , zoals hierboven gedefinieerd, die verantwoordelijk is voor het uitvoeren van clouddiensten op grond van een uitbestedingsovereenkomst.
Clouddiensten	diensten geleverd met behulp van cloudcomputing, dat wil zeggen een model om via het netwerk overal eenvoudig op verzoek toegang te verlenen tot een gedeelde pool van configureerbare IT-middelen (bijvoorbeeld netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald.
Publieke "public" cloud:	cloudinfrastructuur voor vrij gebruik door het algemene publiek.
Private 'privat' cloud:	cloudinfrastructuur voor exclusief gebruik door één onderneming.
Gemeenschappelijke "community" cloud:	cloudinfrastructuur voor exclusief gebruik door een bepaalde community van ondernemingen, bijvoorbeeld meerdere ondernemingen van één groep.
Hybride cloud:	cloudinfrastructuur bestaande uit twee of meer onderscheiden cloudinfrastructuren.

Toepassingsdatum

10. Deze richtsnoeren gelden met ingang van 1 januari 2021 voor alle uitbestedingsovereenkomsten betreffende clouddiensten die op of na deze datum van kracht worden of worden gewijzigd.

11. Ondernemingen moeten bestaande uitbestedingsovereenkomsten betreffende clouddiensten in verband met kritieke of belangrijke operationele functies of activiteiten dienovereenkomstig, indien deze niet voldoen aan deze richtsnoeren, herzien en wijzigen om te zorgen dat zij uiterlijk op 31 december 2022 aan deze richtsnoeren voldoen.

12. Wanneer de herziening van uitbestedingsovereenkomsten betreffende clouddiensten in verband met kritieke of belangrijke functies of activiteiten niet op 31 december 2022 is afgerond, moet de onderneming haar toezichthoudende autoriteit[6] daarvan op de hoogte stellen, met vermelding van de maatregelen die zij heeft gepland om de herziening of de eventuele exitstrategie te voltooien. De toezichthoudende autoriteit kan, indien gepast, met de onderneming een verlengde termijn voor de voltooiing van die herziening overeenkomen.

[6] Artikel 13, lid 10, van de richtlijn Solvabiliteit II.

13. De herziening (indien nodig) van het beleid en de interne processen van de onderneming moet uiterlijk op 1 januari 2021 worden afgerond, terwijl de documentatievereisten voor uitbestedingsovereenkomsten betreffende clouddiensten in verband met kritieke of belangrijke operationele functies of activiteiten uiterlijk op 31 december 2022 moeten worden nageleefd.

Richtsnoer 1 – Clouddiensten en uitbesteding

14. De onderneming moet nagaan of een overeenkomst met een aanbieder van clouddiensten onder de in de richtlijn Solvabiliteit II vastgestelde definitie van uitbesteding valt. Bij deze beoordeling moet worden onderzocht:

a. of de uitbestede operationele functie of activiteit (of een deel daarvan) herhaaldelijk of doorlopend wordt uitgevoerd; en

b. of deze operationele functie of activiteit (of een deel daarvan) normaal gesproken binnen het toepassingsgebied zou vallen van operationele functies of activiteiten die door de onderneming zouden worden of zouden kunnen worden uitgevoerd in het kader van haar gewone bedrijfsactiviteiten, zelfs als de onderneming deze operationele functie of activiteit in het verleden nooit heeft uitgevoerd.

15. Wanneer een overeenkomst met een dienstverlener betrekking heeft op meerdere operationele functies of activiteiten, moet de onderneming bij haar beoordeling rekening houden met alle aspecten van de overeenkomst.

16. Indien de onderneming operationele functies of activiteiten uitbesteedt aan dienstverleners die geen aanbieders van clouddiensten zijn, maar voor de uitvoering van hun diensten wel sterk afhankelijk zijn van cloudinfrastructuren (bijvoorbeeld als de aanbieder van clouddiensten onderdeel is van een onderuitbestedingsketen), valt de overeenkomst betreffende deze uitbesteding binnen het toepassingsgebied van deze richtsnoeren.

Richtsnoer 2 – Algemene beginselen van governance inzake uitbesteding van clouddiensten

17. Onverminderd artikel 274, lid 3, van de gedelegeerde verordening moet het bestuurlijk, beleidsbepalend of toezichthoudend orgaan ((*administrative, management or supervisory body*, hierna "AMSB") van de onderneming ervoor zorgen dat iedere beslissing om kritieke of belangrijke operationele functies of activiteiten uit te besteden aan aanbieders van clouddiensten, gebaseerd is op een grondige risicobeoordeling die zich uitstrekt tot alle relevante risico's die de overeenkomst met zich mee zou kunnen brengen, bijvoorbeeld op het gebied van informatie- en communicatietechnologie (ICT), bedrijfscontinuïteit, juridische en nalevingskwesties, concentratie, overige operationele risico's en risico's in verband met de gegevensmigratie- en/of implementatiefase, voor zover van toepassing.

18. In het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet de onderneming, in voorkomend geval, in haar eigen beoordeling van de risico's en de solvabiliteit (ORSA) rekening houden met de veranderingen in haar risicoprofiel als gevolg van de uitbestedingsovereenkomsten betreffende clouddiensten.

19. Het gebruik van clouddiensten moet in overeenstemming zijn met de strategieën van de onderneming (bijvoorbeeld de ICT-strategie, de informatiebeveiligingsstrategie, de operationeel riskmanagement strategie) alsook

met de interne beleidslijnen en processen, die waar nodig moeten worden geactualiseerd.

Richtsnoer 3 – Actualisering van de schriftelijke beleidslijn inzake uitbesteding

20. In het geval van uitbesteding aan aanbieders van clouddiensten moet de onderneming het schriftelijke uitbestedingsbeleid actualiseren (bijvoorbeeld door deze te herzien, een aparte bijlage toe te voegen of nieuwe specifieke beleidslijnen te ontwikkelen), evenals de overige relevante interne beleidslijnen (bijvoorbeeld op het gebied van informatiebeveiliging). Daarbij moet rekening worden gehouden met de specifieke kenmerken van uitbesteding van clouddiensten en moeten tenminste de volgende punten in acht worden genomen:

a. de rollen en verantwoordelijkheden van de betrokken functies van de onderneming, met name de AMSB, en de afdelingen die verantwoordelijk zijn voor ICT, informatiebeveiliging, naleving, risicobeheer en interne audits;

b. de noodzakelijke processen en verslagleggingsprocedures voor de goedkeuring, de implementatie, de monitoring, het beheer en, in voorkomend geval, de vernieuwing van de uitbestedingsovereenkomsten betreffende clouddiensten in verband met kritieke of belangrijke operationele functies of activiteiten;

c. de controle en monitoring van de clouddiensten, evenredig aan de aard, de omvang en de complexiteit van de inherente risico's van de geleverde diensten, met inbegrip van i) periodieke beoordeling van de risico's van de uitbestedingsovereenkomsten betreffende clouddiensten en een due diligence-onderzoek ten aanzien van de aanbieders van clouddiensten, ii) monitoring- en beheercontroles (bijvoorbeeld controle van de naleving van de service level agreement), en iii) beveiligingsnormen en -controles;

d. met betrekking tot uitbesteding van clouddiensten in verband met kritieke of belangrijke operationele functies of activiteiten moet worden verwezen naar de in richtsnoer 10 bedoelde contractuele bepalingen;

e. documentatievereisten en schriftelijke kennisgeving aan de toezichthouders met betrekking tot uitbesteding van clouddiensten in verband met kritieke of belangrijke operationele functies of activiteiten;

f. voor iedere uitbestedingsovereenkomst betreffende clouddiensten die betrekking heeft op kritieke of belangrijke operationele functies of activiteiten: de verplichte vaststelling van een gedocumenteerde en, waar nodig, naar behoren geteste "exitstrategie" die in verhouding staat tot de aard, de omvang en de complexiteit van de inherente risico's van de geleverde diensten. Deze exitstrategie kan een reeks processen tot beëindiging bevatten, met inbegrip van onder meer stopzetting, reintegratie of overdracht van de diensten waarop de uitbestedingsovereenkomst betreffende clouddiensten betrekking heeft.

Richtsnoer 4 – Schriftelijke kennisgeving aan de toezichthouders

21. De vereisten inzake de schriftelijke kennisgeving als bedoeld in artikel 49, lid 3, van de richtlijn Solvabiliteit II en verder uitgewerkt in de Eiopa-richtsnoeren voor het governancesysteem, zijn van toepassing op alle uitbestedingen van kritieke of belangrijke operationele functies en activiteiten aan aanbieders van clouddiensten. Indien een eerder als niet kritiek of belangrijk aangemerkte uitbestede operationele functie of activiteit kritiek of belangrijk wordt, moet de onderneming de toezichthouders hiervan in kennis stellen.

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

a. een korte beschrijving van de uitbestede operationele functie of activiteit;

b. de aanvangsdatum en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, en de einddatum en/of opzeggingstermijnen voor de aanbieder van clouddiensten en voor de onderneming;

c. het recht dat op de uitbestedingsovereenkomst voor clouddiensten van toepassing is;

d. de naam van de aanbieder van clouddiensten, het bedrijfsregistratienummer, de identificatiecode voor juridische entiteiten (voor zover van toepassing), het geregistreerde adres en andere contactgegevens, de naam van de eventuele moederonderneming en, in het geval van groepen, of de aanbieder van clouddiensten onderdeel is van de groep;

e. cloudservice- en implementatie "deployment" modellen voor de clouddiensten(d.w.z. publiek/privaat/hybride/community), en de specifieke aard van de te bewaren gegevens en de locaties (d.w.z. landen of regio's) waar die gegevens worden opgeslagen;

f. een korte samenvatting van de redenen waarom de uitbestede operationele functie of activiteit kritiek of belangrijk wordt geacht;

g. de datum waarop het kritieke karakter of het belang van de uitbestede operationele functie of activiteit voor het laatst is beoordeeld.

Richtsnoer 5 – documentatievereisten

23. Als onderdeel van haar governance- en risicobeheersysteem moet de onderneming haar uitbestedingsovereenkomsten betreffende clouddiensten documenteren, bijvoorbeeld in de vorm van een speciaal register dat regelmatig wordt bijgewerkt. Ook moet de onderneming gedurende een in overeenstemming met de nationale wetgeving vast te stellen bewaartijd een register bijhouden van beëindigde uitbestedingsovereenkomsten betreffende clouddiensten.

24. In het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten moet de onderneming de volgende informatie bijhouden en vastleggen:

a. de in richtsnoer 4 beschreven informatie waarvan de toezichthouder in kennis moet worden gesteld;

b. in het geval van groepen: de verzekerings- of herverzekeringsondernemingen en de overige binnen het prudentiële consolidatiebereik vallende ondernemingen die van de clouddiensten gebruikmaken;

c. de datum waarop voor het laatst een risicobeoordeling heeft plaatsgevonden, en een korte samenvatting van de belangrijkste resultaten;

d. de persoon of het besluitvormingsorgaan (bijvoorbeeld de AMSB) binnen de onderneming die/dat de uitbestedingsovereenkomst betreffende clouddiensten heeft goedgekeurd;

e. de data van de meest recente en volgende geplande audits, indien van toepassing;

f. de namen van onderaannemers waaraan materiële onderdelen van een kritieke of belangrijke operationele functie of activiteit worden onderuitbesteed, inclusief de landen waar de onderaannemers zijn geregistreerd, waar de dienst

zal worden uitgevoerd en, indien van toepassing, de locaties (d.w.z. landen of regio's) waar de gegevens zullen worden opgeslagen;

g. het resultaat van een beoordeling van de vervangbaarheid van de aanbieder van clouddiensten (bijvoorbeeld eenvoudig, moeilijk of onmogelijk);

h. gegevens met betrekking tot de vraag of de uitbestede kritieke of belangrijke operationele functie of activiteit tijdgevoelige bedrijfsactiviteiten ondersteunt;

i. de geraamde jaarlijkse begrotingskosten;

j. gegevens met betrekking tot de vraag of de onderneming een exitstrategie heeft in het geval van beëindiging van de diensten van een partij of verstoring van de diensten door de aanbieder van clouddiensten.

25. In het geval van uitbesteding van niet-kritieke of niet-belangrijke operationele functies of activiteiten moet de onderneming op basis van de aard, de omvang en de complexiteit van de inherente risico's van de door de aanbieder van clouddiensten verrichte diensten bepalen welke informatie er moet worden bijgehouden.

26. De onderneming moet de toezichthouder op verzoek toegang verlenen tot alle informatie, met inbegrip van een kopie van de uitbestedingsovereenkomst, die deze autoriteit nodig heeft om toezicht te houden op de onderneming.

Richtsnoer 6 – Analyse voorafgaand aan uitbesteding

27. Voordat de onderneming een overeenkomst sluit met een aanbieder van clouddiensten, moet zij:

a. beoordelen of de uitbestedingsovereenkomst betreffende clouddiensten betrekking heeft op een kritieke of belangrijke operationele functie of activiteit in overeenstemming met richtsnoer 7;

b. alle relevante risico's van de uitbestedingsovereenkomst betreffende clouddiensten vaststellen en beoordelen in overeenstemming met richtsnoer 8;

c. een passend due diligence-onderzoek uitvoeren ten aanzien van de mogelijke toekomstige aanbieder van clouddiensten in overeenstemming met richtsnoer 9;

d. belangenconflicten vaststellen en beoordelen die door de uitbesteding kunnen worden veroorzaakt, in overeenstemming met de vereisten van artikel 274, lid 3, onder b), van de gedelegeerde verordening.

Richtsnoer 7 – Beoordeling van kritieke of belangrijke operationele functies en activiteiten

28. Voordat de onderneming een uitbestedingsovereenkomst met een aanbieder van clouddiensten sluit, moet zij beoordelen of deze overeenkomst betrekking heeft op een kritieke of belangrijke operationele functie of activiteit. Bij deze beoordeling moet de onderneming, indien van toepassing, nagaan of de overeenkomst de potentie heeft om in de toekomst kritiek of belangrijk te worden. Ook moet zij het kritieke karakter of het belang van de eerder aan aanbieders van clouddiensten uitbestede operationele functies of activiteiten opnieuw beoordelen als de aard, de omvang en de complexiteit van de inherente risico's van de overeenkomst wezenlijk verandert.

29. Bij de beoordeling moet de onderneming, naast het resultaat van de risicobeoordeling, ten minste rekening houden met de volgende factoren:

a. de mogelijke gevolgen van een wezenlijke verstoring van de uitbestede operationele functie of activiteit of van het ingebreke blijven door de aanbieder

ten aanzien van de overeengekomen service levelsin verband met de clouddiensten, voor de volgende aspecten van de onderneming:

i. de ononderbroken naleving van haar wettelijke verplichtingen;

ii. haar veerkracht en levensvatbaarheid op het gebied van financiën en solvabiliteit op de korte en lange termijn;

iii. de bedrijfscontinuïteit en de operationele veerkracht;

iv. operationele risico's, inclusief gedrags-, ICT- en juridische risico's;

v. reputatierisico;

b. de mogelijke gevolgen van de uitbestedingsovereenkomst betreffende clouddiensten voor het vermogen van de onderneming om:

i. alle relevante risico's vast te stellen, te bewaken en te beheren;

ii. aan alle wettelijke en regelgevingsvereisten te voldoen;

iii. gepaste audits van de uitbestede operationele functie of activiteit uit te voeren;

c. de geaggregeerde blootstelling van de onderneming (en/of de groep, indien van toepassing) aan dezelfde aanbieder van clouddiensten en de mogelijke cumulatieve gevolgen van uitbestedingsovereenkomsten op hetzelfde werkterrein;

d. de omvang en de complexiteit van de werkterreinen van een onderneming die door de uitbestedingsovereenkomst betreffende clouddiensten worden beïnvloed;

e. de mogelijkheid, indien nodig of wenselijk, om de voorgestelde uitbestedingsovereenkomst betreffende clouddiensten over te dragen aan een andere aanbieder van clouddiensten of om de diensten te herintegreren ("vervangbaarheid");

f. de bescherming van persoons- en niet-persoonsgebonden gegevens en de mogelijke gevolgen voor de onderneming, polishouders of andere betrokkenen van een schending van de vertrouwelijkheid of van het niet-waarborgen van de beschikbaarheid en integriteit van gegevens op grond van onder meer Verordening (EU) 2016/679[7]. De onderneming moet in het bijzonder rekening houden met gegevens die bedrijfsgeheimen bevatten en/of gevoelig zijn (bijvoorbeeld gezondheidsgegevens van polishouders).

Richtsnoer 8 – Beoordeling van de risico's van uitbesteding van clouddiensten

30. Over het algemeen moet de onderneming een benadering hanteren die in verhouding staat tot de aard, de omvang en de complexiteit van de inherente risico's van de aan aanbieders van clouddiensten uitbestede diensten. Daartoe behoort ook het beoordelen van de mogelijke gevolgen van de uitbesteding van clouddiensten, in het bijzonder voor de operationele en reputatierisico's.

31. In het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet een onderneming:

[7] 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.

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

b. indien van toepassing en waar nodig, de risico's, waaronder juridische, ICT-, nalevings- en reputatierisico's, en de toezichtsbeperkingen beoordelen die het gevolg zijn van:

   i. de geselecteerde clouddienst en de voorgestelde implementatiemodellen (d.w.z. publiek/privaat/hybride/gemeenschappelijk);

   ii. de migratie en/of deimplementatie);

   iii. de activiteiten en bijbehorende gegevens en systemen die de onderneming overweegt uit te besteden (of die zijn uitbesteed), de gevoeligheid daarvan en de vereiste beveiligingsmaatregelen;

   iv. de politieke stabiliteit en de beveiligingssituatie in de landen (binnen of buiten de EU) waar de uitbestede diensten worden of kunnen worden uitgevoerd en waar de gegevens (waarschijnlijk) worden opgeslagen. Bij de beoordeling moet rekening worden gehouden met:

      1. toepasselijk recht, inclusief wetgeving op het gebied van gegevensbescherming;

      2. de toepasselijke rechtshandhavingsbepalingen;

      3. het insolventierecht dat van toepassing zou zijn bij faillissement van een dienstverlener en de mogelijke beperkingen die zich zouden voordoen bij een urgent herstel van de gegevens van de onderneming;

   v. onderuitbesteding, met inbegrip van de aanvullende risico's die zich kunnen voordoen als de onderaannemer in een derde land of een ander land dan de aanbieder van clouddiensten is gevestigd, alsook het risico dat lange en complexe ketens van onderuitbesteding tot gevolg hebben dat de onderneming haar kritieke of belangrijke operationele functies of activiteiten minder goed kan overzien en controleren en dat de toezichthoudende autoriteiten hierop minder effectief toezicht kunnen houden;

   vi. het algehele risico voor de onderneming van concentratie bij één aanbieder van clouddiensten, met inbegrip van uitbesteding aan een niet gemakkelijk vervangbare aanbieder van clouddiensten of meerdere uitbestedingsovereenkomsten met dezelfde aanbieder van clouddiensten. Bij het beoordelen van het concentratierisico moet de onderneming (en/of de groep, indien van toepassing) rekening houden met al haar uitbestedingsovereenkomsten betreffende clouddiensten met de betreffende aanbieder.

32. De risicobeoordeling moet worden uitgevoerd voordat de onderneming een uitbestedingsovereenkomst betreffende clouddiensten sluit. Als de onderneming aanzienlijke gebreken en/of veranderingen in de dienstverlening of de situatie van de aanbieder van clouddiensten vaststelt, moet de risicobeoordeling onmiddellijk worden herzien of opnieuw worden uitgevoerd. In het geval van wijziging van een

uitbestedingsovereenkomst betreffende clouddiensten met betrekking tot de inhoud en het toepassingsgebied ervan (bijvoorbeeld uitbreiding van het toepassingsgebied of opname van eerder niet opgenomen kritieke of belangrijke operationele functies in het toepassingsgebied) moet de risicobeoordeling opnieuw worden uitgevoerd

Richtsnoer 9 – Due diligence-onderzoek ten aanzien van de aanbieder van clouddiensten

33. De onderneming moet er in haar selectie- en beoordelingsproces voor zorgen dat de aanbieder van clouddiensten geschikt is volgens de in haar schriftelijke beleidslijn inzake uitbesteding beschreven criteria.

34. Het due diligence-onderzoek ten aanzien van de aanbieder van clouddiensten moet voorafgaand aan de uitbesteding van operationele functies of activiteiten worden uitgevoerd. Indien de onderneming een tweede overeenkomst sluit met een reeds beoordeelde aanbieder van clouddiensten, moet zij middels een risicogebaseerde benadering vaststellen of er een tweede due diligence-onderzoek nodig is. Als de onderneming aanzienlijke gebreken en/of veranderingen in de dienstverlening of de situatie van de aanbieder van clouddiensten vaststelt, moet het due diligence-onderzoek onmiddellijk worden herzien of opnieuw worden uitgevoerd.

35. In het geval van uitbesteding van kritieke of belangrijke operationele functies moet in het due diligence-onderzoek een evaluatie van de geschiktheid van de aanbieder van clouddiensten worden opgenomen (bijvoorbeeld vaardigheden, infrastructuur, economische situatie, bedrijfs- en juridischestatus). Indien gepast kan de onderneming ter ondersteuning van het uitgevoerde due diligence-onderzoek gebruikmaken van bewijsmateriaal, certificeringen op basis van internationale normen, auditrapportages van erkende derden of interne auditrapportages.

Richtsnoer 10 – Contractuele bepalingen

36. De respectievelijk rechten en plichten van de onderneming en de aanbieder van clouddiensten moeten duidelijk worden afgebakend en in een schriftelijke overeenkomst worden vastgelegd.

37. Onverminderd artikel 274 van de gedelegeerde verordening moet, in het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten, in de schriftelijke overeenkomst tussen de onderneming en de aanbieder van clouddiensten het volgende worden opgenomen:

a. een duidelijke beschrijving van de uit te voeren uitbestede functies en activiteiten (clouddiensten, met inbegrip van het type dienstverlening);

b. de aanvangsdatum en de einddatum van de overeenkomst, indien van toepassing, en de opzegtermijnen voor de aanbieder van clouddiensten en de onderneming;

c. de bevoegde rechtbank en de wetgeving die op de overeenkomst van toepassing is;

d. de financiële verplichtingen van de partijen;

e. vermelding of de onderuitbesteding van een kritieke of belangrijke operationele functie of activiteit (of wezenlijke delen daarvan) is toegestaan, en, zo ja, welke voorwaarden er van toepassing zijn op de significante onderuitbesteding (zie richtsnoer 13);

f. de locatie(s) (d.w.z. landen of regio's) waar de relevante gegevens zullen worden opgeslagen en verwerkt (locatie van datacentra), en de voorwaarden

waaraan moet worden voldaan, met inbegrip van een verplichting om de onderneming in kennis te stellen als de dienstverlener voorstelt de locatie(s) te wijzigen;

g. bepalingen inzake de toegankelijkheid, beschikbaarheid, integriteit, vertrouwelijkheid, privacy en veiligheid van de relevante gegevens, met inachtneming van de specificaties uit richtsnoer 12;

h. het recht van de onderneming om de prestaties van de aanbieder van clouddiensten regelmatig te monitoren;

i. de overeengekomen niveaus van dienstverlening, die nauwkeurige kwantitatieve en kwalitatieve prestatiedoelen ("KPI's") moeten omvatten om tijdige controle mogelijk te maken, zodat zonder onnodig uitstel passende corrigerende maatregelen kunnen worden genomen indien de overeengekomen "service levels" niet worden gehaald;

j. de rapportageverplichtingen van de aanbieder van clouddiensten aan de onderneming, indien nodig met inbegrip van de verplichtingen om rapportages in te dienen die relevant zijn voor de informatiebeveligingsfunctie en sleutelfuncties van de onderneming, zoals verslagen van de interne-auditfunctie van de aanbieder van clouddiensten;

k. vermelding of de aanbieder van clouddiensten zich verplicht tegen bepaalde risico's moet verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking;

l. vereisten inzake de invoering en het testen van bedrijfscontinuïteitsplannen ("BCP's");

m. de verplichting voor de aanbieder van clouddiensten om de onderneming, haar toezichthouders en iedere andere door de onderneming of de toezichthouders aangestelde persoon de volgende rechten te verlenen:

    i. volledige toegang tot alle relevante bedrijfslocaties (hoofdkantoren en operationele centra), inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestedefunctie of activiteit uit te voeren, waaronder bijbehorende financiële informatie, personeel en de externe auditors van de aanbieder van clouddiensten ("toegangsrecht");

    ii. een onbeperkt recht van onderzoek en audits met betrekking tot de uitbestedingsovereenkomst betreffende clouddiensten ("onderzoeks en auditrecht") om hen in staat te stellen de uitbestedingsovereenkomst te controleren en ervoor te zorgen dat aan alle toepasselijke regelgeving en contractuele bepalingen wordt voldaan;

n. bepalingen om ervoor te zorgen dat de onderneming haar gegevens onmiddellijk kan herstellen in het geval van insolvabiliteit, liquidatie of beëindiging van de bedrijfsactiviteiten van de aanbieder van clouddiensten.

Richtsnoer 11 – Toegangs- en auditrecht

38. De uitbestedingsovereenkomst voor clouddiensten mag de effectieve uitoefening van het toegangs- en auditrecht van de onderneming en haar toezichthouders en de mogelijkheden tot controle van de clouddiensten om aan haar wettelijke verplichtingen te voldoen, niet beperken.

39. De onderneming moet haar toegangs- en auditrecht uitoefenen en de auditfrequentie en de middels een op risico gebaseerde benadering te controleren gebieden en diensten vastleggen overeenkomstig punt 8 van de Eiopa-richtsnoeren voor het governancesysteem.

40. Bij het bepalen van de frequentie en de reikwijdte van de uitoefening van haar toegangs- of auditrecht moet de onderneming in overweging nemen of de uitbesteding van clouddiensten verband houdt met een kritieke of belangrijke operationele functie of activiteit. Ook moet zij rekening houden met de aard en omvang van het risico en met de gevolgen van de uitbestedingsovereenkomst betreffende clouddiensten voor de onderneming.

41. Als de uitoefening van haar toegangs- of auditrecht of het gebruik van bepaalde audittechnieken een risico oplevert voor de omgeving van de aanbieder van clouddiensten en/of een andere klant van de aanbieder van clouddiensten (bijvoorbeeld de gevolgen voor de dienstverleningsniveaus, de beschikbaarheid van gegevens, vertrouwelijkheidsaspecten), moeten de onderneming en de aanbieder van clouddiensten alternatieve manieren overeenkomen om een vergelijkbaar niveau van betrouwbaarheid en dienstverlening voor de onderneming te verwezenlijken (bijvoorbeeld de opname van specifieke controles die worden getest in het kader van een specifiek verslag/specifieke certificering van de aanbieder van clouddiensten).

42. Onverminderd hun eindverantwoordelijkheid ten aanzien van de door hun aanbieders van clouddiensten uitgevoerde activiteiten kunnen ondernemingen, om hun auditmiddelen efficiënter aan te wenden en de organisatorische last voor de aanbieder van clouddiensten en zijn klanten te verlichten, gebruikmaken van:

a. door de aanbieder van clouddiensten verstrekte externe certificeringen en externe of interne auditrapportages;

b. gemeenschappelijke audits (d.w.z. audits die samen met andere klanten van dezelfde aanbieder van clouddiensten worden uitgevoerd), of door een door hen aangestelde derde uitgevoerde gemeenschappelijke audits.

43. In het geval van uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies of activiteiten mogen ondernemingen alleen gebruikmaken van de in punt 42, onder a), genoemde methode als zij:

a. erop toezien dat de certificering of de auditrapportage betrekking heeft op de door de onderneming vastgestelde systemen (bijvoorbeeld processen, applicaties, infrastructuur, datacentra enz.) en controles, en de naleving van de relevante vereisten beoordelen;

b. de inhoud van nieuwe certificeringen of auditrapportages regelmatig grondig beoordelen en nagaan of de certificeringen of rapportages niet verouderd zijn;

c. erop toezien dat ook toekomstige versies van de certificering of het auditrapport betrekking hebben op essentiële systemen en controles;

d. zich hebben vergewist van de geschiktheid van de certificerende of controlerende partij (bijvoorbeeld met betrekking tot roulering van de certificerende of controlerende organisatie, kwalificaties, deskundigheid, herhaling van de uitvoering/controle van bewijsstukken in het betrokken auditdossier);

e. zich ervan hebben vergewist dat er certificeringen zijn afgegeven, dat de audits zijn uitgevoerd overeenkomstig gepaste normen en dat deze een toetsing omvatten van de operationele doeltreffendheid van de aanwezige essentiële controles;

f. contractueel gerechtigd zijn te verzoeken om uitbreiding van de reikwijdte van de certificeringen of auditrapportages tot andere relevante systemen en controles, 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 behouden om naar eigen inzicht individuele audits op locatie uit te voeren ten aanzien van de uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies of activiteiten; dit recht moet worden uitgeoefend in geval van specifieke behoeften waarin niet via andere soorten interactie met de aanbieder van clouddiensten kan worden voorzien.

44. Wat betreft de uitbesteding van kritieke of belangrijke operationele functies aan aanbieders van clouddiensten moeten ondernemingen beoordelen of de externe certificeringen en rapportages als bedoeld in punt 42, onder a), adequaat zijn en volstaan om aan hun uit de regelgeving voortvloeiende verplichtingen te voldoen, en dienen zij, in het kader van een risicogebaseerde benadering, niet uitsluitend op deze verslagen en certificeringen te vertrouwen.

45. Voorafgaand aan een gepland locatiebezoek moet de partij die gebruik wil maken van haar toegangsrecht (onderneming, auditor of namens de onderneming(en) handelende derde), een redelijke termijn in acht nemen om kennis te geven van dit voornemen, tenzij tijdige kennisgeving vanwege een nood- of crisissituatie niet mogelijk is. In deze kennisgeving moeten de locatie en het doel van het bezoek worden vermeld, evenals het personeel dat aan het bezoek zal deelnemen.

46. Aangezien cloudoplossingen technisch bijzonder complex zijn, moet de onderneming zich ervan vergewissen dat het personeel dat de audit verricht – haar eigen interne auditors of de namens haar handelende pool van auditors dan wel de door de aanbieder van clouddiensten aangestelde auditors, c.q. het personeel dat de externe certificering of de auditrapportages van de aanbieder evalueert, over de juiste vaardigheden en kennis beschikt om de betreffende audits en/of beoordelingen te verrichten.

Richtsnoer 12 – Beveiliging van gegevens en systemen

47. De onderneming moet ervoor zorgen dat aanbieders van clouddiensten de Europese en nationale regelgeving en gepaste ICT-beveiligingsnormen naleven.

48. In het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet de onderneming daarnaast specifieke informatiebeveiligingseisen opnemen in de uitbestedingsovereenkomst en de naleving van deze eisen regelmatig monitoren.

49. Met het oog op punt 48 moet de onderneming, in het geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten, middels een risicogebaseerde benadering en met inachtneming van haar eigen verantwoordelijkheden en die van de aanbieder van clouddiensten:

a. afspraken maken over een duidelijke verdeling van taken en verantwoordelijkheden tussen de aanbieder van clouddiensten en de onderneming met betrekking tot de operationele functies of activiteiten die door de uitbesteding van clouddiensten worden beïnvloed;

b. een passend beschermingsniveau voor de vertrouwelijkheid van gegevens, de continuïteit van de uitbestede activiteiten en de integriteit en herleidbaarheid van gegevens en systemen in het kader van de voorgenomen uitbesteding definiëren en desbetreffende besluiten vaststellen;

c. nagaan of er specifieke maatregelen nodig zijn voor gegevens in transit, opgeslagen gegevens in het geheugen en gegevens in rusttoestand, bijvoorbeeld de toepassing van versleutelingstechnieken (encryptie) in combinatie met een passend sleutelbeheer;

d. aandacht besteden aan de mechanismen voor integratie van de clouddiensten in de systemen van de onderneming, bijvoorbeeld de programmeringsinterfaces van applicaties en een goed gebruikers- en toegangsbeheerproces;

e. contractueel vastleggen dat de beschikbaarheid van netwerkverkeer en de verwachte capaciteit aan strenge continuïteitseisen moeten voldoen, indien van toepassing en haalbaar;

f. gepaste continuïteitseisen definiëren en desbetreffende besluiten vaststellen om te zorgen voor adequate continuïteit op ieder niveau van de technologische keten, indien van toepassing;

g. over een gedegen en goed gedocumenteerd incidentenbeheerproces beschikken, met inbegrip van de verantwoordelijkheden van beide partijen, bijvoorbeeld door vaststelling van een samenwerkingsmodel in geval van daadwerkelijke of vermoede incidenten;

h. een risicogebaseerde benadering van met betrekking tot de locatie(s) (d.w.z. land of regio) voor gegevensopslag en -verwerking en met betrekking tot informatiebeveiliging hanteren;

i. de naleving monitoren van de eisen ten aanzien van de effectiviteit en efficiëntie van de door de aanbieder van clouddiensten geïmplementeerde controlemechanismen waarmee wordt beoogd de risico's in verband met de verrichte diensten te beperken.

Richtsnoer 13 – Onderuitbesteding van kritieke of belangrijke operationele functies en activiteiten

50. Indien onderuitbesteding van kritieke of belangrijke operationele functies (of een deel daarvan) is toegestaan, moet(en) in de uitbestedingsovereenkomst voor clouddiensten tussen de onderneming en de aanbieder van clouddiensten:

a. alle soorten activiteiten worden vermeld die van potentiële onderuitbesteding zijn uitgesloten;

b. de voorwaarden worden vermeld waaraan moet worden voldaan in geval van onderuitbesteding (bijvoorbeeld dat de onderaannemer de relevante verplichtingen van de aanbieder van clouddiensten ook volledig moet naleven). Deze verplichtingen omvatten ook het audit-, onderzoeks- en toegangsrecht en de beveiliging van gegevens en systemen;

c. worden vermeld dat de aanbieder van clouddiensten volledig aansprakelijk blijft en de onderuitbestede diensten moet monitoren en controleren;

d. een verplichting worden opgenomen voor de aanbieder van clouddiensten om de onderneming in kennis te stellen van alle voorgenomen belangrijke wijzigingen van de onderaannemers of in onderuitbesteding gegeven diensten die ertoe zouden kunnen leiden dat de aanbieder minder goed in staat is zijn verplichtingen uit hoofde van de uitbestedingsovereenkomst voor clouddiensten na te komen. De kennisgevingstermijn voor dergelijke wijzigingen moet de uitbestedende instelling minimaal in staat stellen de risico's als gevolg van de voorgestelde wijzigingen van de onderaannemers of de in

onderuitbesteding gegeven diensten te beoordelen voordat deze daadwerkelijk van kracht worden;

e. worden gewaarborgd dat de onderneming, als een aanbieder van clouddiensten wijzigingen van een onderaannemer of in onderuitbesteding gegeven diensten plant die nadelig zouden zijn voor het risicoprofiel van de overeengekomen diensten, het recht heeft bezwaar te maken tegen deze wijzigingen en/of de overeenkomst te beëindigen en het contract op te zeggen.

Richtsnoer 14 – Monitoring van en controle op uitbestedingsovereenkomsten betreffende clouddiensten

51. De onderneming moet regelmatig de prestaties van activiteiten, de beveiligingsmaatregelen en de naleving van het overeengekomen dienstverleningsniveauvan haar aanbieders van clouddiensten monitoren middels een risicogebaseerde benadering. Daarbij moet het accent liggen op de uitbesteding van clouddiensten voor kritieke en belangrijke operationele functies.

52. De onderneming moet daarvoor monitoring- en controlemechanismen creëren, waarbij, indien haalbaar en gepast, rekening moet worden gehouden met eventuele onderuitbesteding van kritieke of belangrijke operationele functies of een deel daarvan.

53. Het AMSB moet periodiek op de hoogte worden gebracht van de vastgestelde risico's van de uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies en activiteiten.

54. Om te zorgen voor adequate monitoring van en controle op hun uitbestedingsovereenkomsten betreffende clouddiensten moeten ondernemingen voldoende personeel inzetten dat over voldoende vaardigheden en kennis beschikt om de naar de cloud uitbestede diensten te monitoren. Het personeel van de onderneming dat met deze activiteiten is belast, moet, wanneer dit nodig wordt geacht, zowel over ICT- als over bedrijfskennis beschikken.

Richtsnoer 15 – Beëindigingsrecht en exitstrategieën

55. In het geval van uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies of activiteiten moet de onderneming een duidelijk gedefinieerde exitstrategieclausule in de uitbestedingsovereenkomst voor clouddiensten opnemen om ervoor te zorgen dat zij de overeenkomst indien nodig kan beëindigen. Deze beëindiging moet mogelijk worden gemaakt zonder afbreuk te doen aan de continuïteit en kwaliteit van haar dienstverlening voor polishouders. Daartoe moet de onderneming:

a. exitplannen ontwikkelen die volledig, servicegericht, gedocumenteerd en naar behoren getest zijn (bijvoorbeeld door middel van een analyse van de potentiële kosten, gevolgen, middelen en implicaties voor de tijdsplanning van verschillende potentiële exit-alternatieven);

b. alternatieve oplossingen zoeken en passende en haalbare overgangsplannen ontwikkelen waarmee zij bestaande activiteiten en gegevens bij de aanbieder van clouddiensten kan weghalen en naar alternatieve aanbieders of aan de onderneming zelf kan overdragen. Deze oplossingen moeten worden vastgesteld met het oog op de uitdagingen die zich kunnen voordoen in verband met de locatie van de gegevens, en daarbij moeten de nodige maatregelen worden genomen om de bedrijfscontinuïteit tijdens de overgangsfase te waarborgen;

c. ervoor zorgen dat de aanbieder van clouddiensten de onderneming adequaat ondersteunt bij het overbrengen van de uitbestede gegevens, systemen of applicaties naar een andere aanbieder of rechtstreeks naar de onderneming;

d. met de aanbieder van clouddiensten overeenkomen dat deze de gegevens van de onderneming in alle regio's volledig en op veilige wijze verwijdert nadat deze weer aan de onderneming zijn overgedragen.

56. Bij het ontwikkelen van een exitstrategie moet de onderneming aandacht besteden aan:

a. vaststelling van de doelen van de exitstrategie;

b. vaststelling van de gebeurtenissen (bijvoorbeeld de belangrijkste risico-indicatoren waaruit een onaanvaardbaar niveau van dienstverlening blijkt) waardoor de exitstrategieclausule n werking wordt gesteld;

c. effectbeoordeling van de potentiële bedrijfsschade in verhouding tot de uitbestede activiteiten om na te gaan welke personele en andere middelen er nodig zouden zijn om het exitplan uit te voeren en hoe lang dat zou duren;

d. toewijzing van taken en verantwoordelijkheden voor het beheer van exitplannen en overgangsactiviteiten;

e. opstelling van criteria om te bepalen of de overgang is geslaagd.

Richtsnoer 16 – Toezicht op uitbestedingsovereenkomsten betreffende clouddiensten door toezichthoudende autoriteiten

57. Als onderdeel van hun toetsingsproces dienen toezichthoudende autoriteiten , een analyse te verrichten van de gevolgen van de door ondernemingen gesloten uitbestedingsovereenkomsten betreffende clouddiensten. Deze analyse moet met name gericht zijn op overeenkomsten die verband houden met de uitbesteding van kritieke of belangrijke operationele functies of activiteiten.

58. Toezichthoudende autoriteiten moeten bij het toezicht op de uitbestedingsovereenkomsten betreffende clouddiensten van ondernemingen rekening houden met de volgende risico's:

a. ICT-risico's;

b. andere operationele risico's (met inbegrip van juridische en nalevingsrisico's en risico's in verband met uitbesteding en beheer van derden);

c. reputatierisico;

d. concentratierisico's, ook op nationaal/sectoraal niveau.

59. In hun beoordeling dienen de toezichthoudende autoriteiten in het kader van een risicogebaseerde benadering aandacht te besteden aan de volgende aspecten:

a. de gepastheid en effectiviteit van de governance- en operationele processen van de onderneming op het gebied van goedkeuring, implementatie, monitoring, beheer en vernieuwing van uitbestedingsovereenkomsten betreffende clouddiensten;

b. de vraag of de onderneming over voldoende middelen beschikt, met toereikende vaardigheden en kennis voor de monitoring van de naar de cloud uitbestede diensten;

c. de vraag of de onderneming alle in deze richtsnoeren genoemde risico's vaststelt en beheert.

60. In het geval van groepen moet de groepstoezichthouder ervoor zorgen dat de gevolgen van de uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies of activiteiten in aanmerking worden genomen in de groepsrisicobeoordeling, met inachtneming van de eisen uit de punten 58 en 59 en de individuele governance- en operationele kenmerken van de groep.

61. Als er meerdere ondernemingen in verschillende lidstaten betrokken zijn bij de uitbesteding van clouddiensten voor kritieke of belangrijke operationele functies of activiteiten en deze uitbesteding centraal door de moederonderneming of een dochteronderneming uit de groep (bijvoorbeeld een onderneming of een dienstverlener van de groep, zoals de ICT-dienstverlener van de groep) wordt beheerd, moet(en) de groepstoezichthouder en/of de relevante toezichthoudende autoriteiten van de bij de uitbesteding van clouddiensten betrokken ondernemingen, indien van toepassing, de gevolgen van de uitbesteding van clouddiensten voor het risicoprofiel van de groep aan de orde stellen in het college van toezichthouders.

62. Wanneer wordt vastgesteld dat er punten van zorg zijn die tot de conclusie leiden dat een onderneming niet langer solide governanceregelingen heeft of niet aan de regelgevingsvereisten voldoet, moeten de toezichthoudende autoriteiten passende maatregelen nemen, bijvoorbeeld door de onderneming te verplichten de governanceregeling te verbeteren, de reikwijdte van de uitbestede functies te beperken of door opzegging van een of meer uitbestedingsovereenkomsten te eisen. In het bijzonder kan, aangezien de continuïteit van de werkzaamheden van de onderneming moet worden gewaarborgd, de ontbinding van contracten worden verlangd als het toezicht op en de handhaving van de regelgevingsvereisten niet via andere maatregelen kan worden bewerkstelligd.

Regels inzake naleving en rapportage

63. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1094/2010. Overeenkomstig artikel 16, lid 3, van die verordening moeten de bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan de richtsnoeren en aanbevelingen te voldoen.

64. Bevoegde autoriteiten die aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, moeten deze op een passende manier integreren in hun wetgevend of toezichthoudend kader.

65. Bevoegde autoriteiten moeten binnen twee maanden na publicatie van de vertaalde versies aan Eiopa bevestigen of zij voldoen of voornemens zijn te voldoen aan deze richtsnoeren. Indien zij er niet aan voldoen of niet voornemens zijn eraan te voldoen, moeten zij de Autoriteit daarvan in kennis stellen, met opgave van de redenen.

66. Bij uitblijven van een antwoord binnen deze termijn worden de bevoegde autoriteiten geacht niet te voldoen aan de rapportageverplichting en zal hiervan melding worden gedaan.

Slotbepaling inzake herziening

67. Deze richtsnoeren kunnen door Eiopa worden herzien.