EIOPA-BoS-20-002

Retningslinjer for outsourcing til cloududbydere

Indhold

Indledning

1. I henhold til artikel 16 i forordning (EU) nr. 1094/2010[1] udsteder EIOPA retningslinjer og henstillinger til forsikrings- og genforsikringsselskaber om, hvordan bestemmelserne om outsourcing i direktiv 2009/138/EF[2] ("Solvens II-direktivet") og i Kommissionens delegerede forordning (EU) nr. 2015/35[3] ("den delegerede forordning") skal anvendes i tilfælde af outsourcing til cloududbydere.

2. Disse retningslinjer er baseret på artikel 13, nr. 28, 38 og 49 i Solvens II-direktivet, og artikel 274 i den delegerede forordning. Derudover bygger disse retningslinjer på EIOPA's "Retningslinjer for ledelsessystem" (EIOPA-BoS-14/253).

3. Disse retningslinjer er rettet til de kompetente myndigheder med henblik på at vejlede om, hvordan forsikrings- og genforsikringsselskaber (i fællesskab betegnet "selskab(er)") bør anvende de krav vedrørende outsourcing, der er fastsat i ovennævnte retsakter i forbindelse med outsourcing til cloududbydere.

4. Retningslinjerne gælder både for enkeltselskaber og tilsvarende for koncerner[4].

   Enheder, der er omfattet af andre sektorspecifikke krav og er en del af en koncern, er på individuelt niveau ikke omfattet af disse retningslinjer, da de skal følge de sektorspecifikke krav samt de pågældende retningslinjer udstedt af Den Europæiske Værdipapir- og Markedstilsynsmyndighed og Den Europæiske Banktilsynsmyndighed.

5. Ved outsourcing og videreoutsourcing til cloududbydere inden for koncernen bør disse retningslinjer anvendes sammen med bestemmelserne i EIOPA's "Retningslinjer for ledelsessystem" om outsourcing inden for koncernen.

6. Selskaber og kompetente myndigheder bør, når de efterlever eller fører tilsyn med overholdelsen af disse retningslinjer, tage hensyn til proportionalitetsprincippet[5] og den kritiske karakter eller vigtigheden af den tjeneste, der er outsources til cloududbydere. Proportionalitetsprincippet bør sikre, at ledelsesmæssige foranstaltninger, herunder de, der vedrører outsourcing til cloududbydere, står i rimeligt forhold til arten, omfanget og kompleksiteten af de underliggende risici.

7. Disse retningslinjer bør læses sammen med og med forbehold af EIOPA's "Retningslinjer for ledelsessystem" og af de lovfæstede forpligtelser, der er anført i pkt. 1.

Definitioner

8. For begreber, der ikke er defineret i disse retningslinjer, er betydningen den, der er fastlagt i de retsakter, der henvises til i indledningen.

9. I disse retningslinjer finder endvidere følgende definitioner anvendelse:

Tjenesteyder	en tredjepartsenhed, der udfører en procedure, tjenesteydelse eller aktivitet eller dele deraf under en outsourcingaftale.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EFT L 331 af 15.12.2010, s. 48).

[2] Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EFT L 335 af 17.12.2009, s. 1).

[3] Kommissionens delegerede forordning (EU) 2015/35 af 10. oktober 2014, der supplerer Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 12 af 17.1.2015, s. 1).

[4] Artikel 212, stk. 1, i Solvens II-direktivet.

[5] Artikel 29, stk. 3, i Solvens II-direktivet.

Cloududbyder	en tjenesteyder som defineret ovenfor, der er ansvarlig for at levere cloudtjenester i henhold til en outsourcingaftale.
Cloudtjenester	tjenesteydelser leveret ved hjælp af cloudcomputing, dvs. en model for lettilgængelig og letanvendelig on demand-netværksadgang til en fælles pulje af konfigurerbare computerressourcer (f.eks. netværk, servere, lagring, applikationer og serviceydelser), som hurtigt kan leveres og idriftsættes med et minimum af administration eller interaktion med tjenesteyderen.
Offentlig cloud	cloudinfrastruktur, som er gratis tilgængelig for offentligheden.
Privat cloud	cloudinfrastruktur, som udelukkende kan anvendes af ét enkelt selskab.
Fælles cloud	cloudinfrastruktur, som udelukkende er tilgængelig for en bestemt gruppe selskaber, f.eks. selskaber i én enkelt koncern.
Hybrid cloud	cloudinfrastruktur, som er sammensat af to eller flere særskilte cloudinfrastrukturer.

Anvendelsesdato

10. Disse retningslinjer finder anvendelse fra den 1. januar 2021 på alle cloud-outsourcingaftaler, der indgås eller ændres på denne dato eller efterfølgende.

11. Eksisterende cloud-outsourcingaftaler, der vedrører kritiske eller vigtige operationelle funktioner eller aktiviteter, bør selskaberne gennemgå og ændre tilsvarende for at sikre overholdelse af disse retningslinjer senest 31. december 2022.

12. Er gennemgangen af aftalerne om outsourcing af kritiske eller vigtige funktioner ikke afsluttet senest 31. december 2022, bør selskabet underrette sin tilsynsmyndighed herom[6], herunder om de foranstaltninger, der er planlagt for at fuldføre gennemgangen eller den mulige exit-strategi. Tilsynsmyndigheden kan aftale en forlænget tidsfrist med selskabet for gennemførelse af denne gennemgang, hvis det er hensigtsmæssigt.

13. En eventuel nødvendig ajourføring af selskabets politikker og interne processer bør være foretaget senest 1. januar 2021, mens dokumentationskravene til cloud-outsourcingaftaler vedrørende kritisk eller vigtige operationelle funktioner eller aktiviteter bør være gennemført senest 31. december 2022.

[6] Artikel 13, stk. 10, i Solvens II-direktivet.

Retningslinje 1 – cloudtjenester og cloudoutsourcing

14. Selskabet bør vurdere, om en aftale med en cloududbyder falder ind under definitionen af outsourcing i henhold til Solvens II-direktivet. Ved vurderingen heraf bør der tages hensyn til:

a. hvorvidt den outsourcede operationelle funktion eller aktivitet (eller en del deraf) udføres på tilbagevendende eller løbende basis, og

b. hvorvidt denne operationelle funktion eller aktivitet (eller en del deraf) normalt vil falde ind under operationelle funktioner eller aktiviteter, som selskabet ville eller kunne udføre som led i sine normale forretningsaktiviteter, også hvis selskabet ikke tidligere har udøvet denne operationelle funktion eller aktivitet.

15. Hvis en aftale med en tjenesteyder omfatter flere operationelle funktioner eller aktiviteter, bør selskabet tage alle aspekter af aftalen i betragtning i sin vurdering.

16. I tilfælde, hvor selskabet outsourcer operationelle funktioner eller aktiviteter til tjenesteydere, som ikke er cloududbydere, men i stort omfang forlader sig på cloudinfrastrukturer for at levere deres tjenester (f.eks. når cloududbyderen er et led i en videreoutsourcingkæde), falder outsourcingaftalen ind under anvendelsesområdet for disse retningslinjer.

Retningslinje 2 – generelle principper for styring af cloudoutsourcing

17. Med forbehold af artikel 274, stk. 3, i den delegerede forordning bør selskabets administrations-, ledelses- eller tilsynsorgan ("AMSB") sikre, at enhver beslutning om at outsource kritiske eller vigtige operationelle funktioner eller aktiviteter til cloududbydere baseres på en grundig risikovurdering, herunder af alle relevante risici, der er forbundet med arrangementet, såsom risici vedrørende informations- og kommunikationsteknologi (IKT), forretningskontinuitet, juridiske forhold og regelefterlevelse, koncentration, andre operationelle risici, og risici vedrørende datamigration og/eller gennemførelsesfasen, når det er relevant.

18. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter til cloududbydere bør ændringer i selskabets risikoprofil som følge af dets cloud-outsourcingaftaler afspejles i selskabets vurdering af egen risiko og solvens ("ORSA"), hvor det er relevant.

19. Brugen af cloudtjenester bør være i overensstemmelse med selskabets strategier (f.eks. IKT-strategi, strategi for informationssikkerhed, strategi for styring af operationelle risici) og interne politikker og processer, som om nødvendigt bør ajourføres.

Retningslinje 3 – ajourføring af den skriftlige politik for outsourcing

20. Ved outsourcing til cloududbydere bør selskabet ajourføre den skriftlige politik for outsourcing (f.eks. ved at gennemgå den, tilføje et særskilt tillæg eller udvikle nye målrettede politikker) og de andre relevante interne politikker (f.eks. informationssikkerhed), for at tage hensyn til særlige forhold vedrørende cloudoutsourcing, i det mindste på følgende områder:

a. rollerne og ansvarsområderne for selskabets involverede funktioner, navnlig administrations-, ledelses- eller tilsynsorganet (AMSB) og funktioner med ansvar for IKT, informationssikkerhed, regelefterlevelse, risikostyring og intern revision

b. de processer og rapporteringsprocedurer, der er nødvendige for godkendelse, gennemførelse, overvågning, styring og i givet fald fornyelse af cloud-

outsourcingaftaler vedrørende kritiske eller vigtige operationelle funktioner eller aktiviteter

c. tilsynet med cloudtjenester i rimeligt forhold til arten, omfanget og kompleksiteten af de iboende risici ved de leverede tjenester, herunder i) risikovurdering af cloud-outsourcingaftaler og due diligence for cloududbydere, herunder hyppigheden af risikovurderingen, (ii) kontroller til overvågning og styring (f.eks. verifikation af serviceleveranceaftalen) og (iii) sikkerhedsstandarder og -kontroller

d. for outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter bør der henvises til de kontraktlige krav som beskrevet i retningslinje 10

e. dokumentationskrav og skriftlig underretning af tilsynsmyndigheden om cloudoutsourcing vedrørende kritiske eller vigtige operationelle funktioner eller aktiviteter

f. for hver cloud-outsourcingaftale, der omfatter kritiske eller vigtige operationelle funktioner eller aktiviteter, et krav om en dokumenteret og, når det hensigtsmæssigt, tilstrækkeligt afprøvet "exit-strategi", som står i rimeligt forhold til arten, omfanget og kompleksiteten af de iboende risici ved de leverede tjenester. Exit-strategien kan omfatte en række afslutningsprocesser, herunder, men ikke nødvendigvis begrænset til, ophør, reintegration eller overførsel af de tjenester, der er omfattet af aftalen om cloudoutsourcing.

Retningslinje 4 – skriftlig underretning af tilsynsmyndigheden

21. Kravene om skriftlig underretning i artikel 49, stk. 3, i Solvens II-direktivet og nærmere beskrevet i EIOPA's "Retningslinjer for ledelsessystem" finder anvendelse på enhver outsourcing af kritiske eller vigtige operationelle funktioner og aktiviteter til cloududbydere. Hvis en outsourcet operationel funktion eller aktivitet, der tidligere er klassificeret som ikke-kritisk eller ikke-vigtig, bliver kritisk eller vigtig, bør selskabet underrette tilsynsmyndigheden herom.

22. Selskabets skriftlige underretning bør under hensyntagen til proportionalitetsprincippet mindst omfatte følgende oplysninger:

a. en kort beskrivelse af den outsourcede operationelle funktion eller aktivitet

b. startdato og, i givet fald, dato for næste kontraktfornyelse, slutdato og/eller opsigelsesvarsel for cloududbyderen og for selskabet

c. den gældende lovgivning for aftalen om cloudoutsourcing

d. navnet på cloududbyderen, selskabets registreringsnummer, den juridiske identifikationskode (LEI) (hvis den foreligger), den registrerede adresse og andre relevante kontaktoplysninger samt navnet på dets eventuelle moderselskab og, for koncerner, hvorvidt cloududbyderen er en del af koncernen eller ej

e. cloudtjenesterne og implementerigsmodellerne (dvs. offentlig/privat/hybrid/fælles), den specifikke art af de data, der skal opbevares, samt de steder (dvs. lande eller regioner), hvor dataene vil blive opbevaret

f. en kort sammenfatning af begrundelsen for, at den outsourcede operationelle funktion eller aktivitet anses for kritisk eller vigtig

g. datoen for den seneste vurdering af den outsourcede funktions kritiske eller vigtige karakter.

Retningslinje 5 – krav til dokumentation

23. Selskabet bør som led i sit ledelses- og risikostyringssystem registrere sine cloud-outsourcingaftaler, f.eks. i et særligt register, der løbende holdes ajour. Selskabet bør desuden føre et register over ophørte cloud-outsourcingaftaler i en opbevaringsperiode, der er fastlagt i national lovgivning.

24. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter bør selskabet registrere alle følgende oplysninger:

a. de oplysninger, der skal meddeles til tilsynsmyndigheden, som anført i retningslinje 4

b. for koncerner, de forsikrings- eller genforsikringsselskaber og andre selskaber, der er omfattet af konsolideringsreglerne, og som gør brug af cloudtjenester

c. datoen for den seneste risikovurdering, og en kort oversigt over de vigtigste resultater

d. den person eller det beslutningstagende organ (f.eks. administrations-, ledelses- eller tilsynsorganet (AMSB)) i selskabet, som har godkendt cloudoutsourcingaftalen

e. datoerne for de seneste og, i givet fald, planlagte næste revisioner

f. hvis det er relevant, navnene på eventuelle underkontrahenter, til hvem væsentlige dele af en kritisk eller vigtig funktion er videreoutsourcet, herunder de lande, hvor underkontrahenterne er registreret, hvor tjenesten vil blive ydet, og, i givet fald, de steder (dvs. de lande eller regioner), hvor dataene vil blive opbevaret

g. en vurdering af, hvor let cloududbyderen kan erstattes (f.eks. let, vanskeligt eller umuligt)

h. hvorvidt de outsourcede kritiske eller vigtige operationelle funktioner eller aktiviteter understøtter tidskritisk forretningsdrift

i. den anslåede årlige budgetbelastning

j. hvorvidt selskabet har en exit-strategi i tilfælde af, at en af parterne opsiger kontrakten, eller at tjenesteydelserne fra cloududbyderen afbrydes.

25. I tilfælde af outsourcing af ikke-kritiske eller ikke-vigtige operationelle funktioner eller aktiviteter bør selskabet definere, hvilke oplysninger der skal registreres, på grundlag af arten, omfanget og kompleksiteten af de iboende risici ved de tjenester, der leveres af cloududbyderen.

26. Selskabet bør på anmodning fra tilsynsmyndigheden stille alle oplysninger til rådighed, der er nødvendige for myndighedens tilsyn med selskabet, herunder en kopi af outsourcingaftalen.

Retningslinje 6 – analyse forud for outsourcing

27. Før der indgås nogen aftale med cloududbydere, bør selskabet:

a. vurdere, om cloud-outsourcingaftalen vedrører en kritisk eller vigtig operationel funktion eller aktivitet i henhold til retningslinje 7

b. afdække og vurdere alle de relevante risici ved cloud-outsourcingaftalen i overensstemmelse med retningslinje 8

c. foretage passende due diligence for den potentielle cloududbyder i overensstemmelse med retningslinje 9

d. identificere og vurdere interessekonflikter, som outsourcingen kan medføre, i henhold til kravene i artikel 274, stk. 3, litra b), i den delegerede forordning.

Retningslinje 7 – vurdering af kritiske eller vigtige operationelle funktioner og aktiviteter

28. Før selskabet indgår en aftale om outsourcing med cloududbydere bør det vurdere, om cloud-outsourcingaftalen vedrører en kritisk eller vigtig operationel funktion eller aktivitet. Ved denne vurdering bør selskabet, hvor det er relevant, overveje, om aftalen har potentiale til i fremtiden at blive kritisk eller vigtig. Såfremt arten, omfanget og kompleksiteten af de iboende risici ved aftalen ændrer sig væsentligt, bør selskabet desuden foretage en ny vurdering af den kritiske karakter eller vigtigheden af den operationelle funktion eller aktivitet, derer outsourcet til cloududbydere.

29. Ved vurderingen bør selskabet som minimum tage hensyn til følgende faktorer foruden resultatet af risikovurderingen:

a. mulige konsekvenser af enhver væsentlig afbrydelse af den outsourcede operationelle funktion eller aktivitet, eller cloududbyderens manglende evne til at levere tjenesterne på det aftalte serviceniveau i forhold til selskabets:
    i. fortsatte opfyldelse af sine lovbestemte forpligtelser
    ii. kort- og langsigtede finansielle situation, solvenssituation, solvensmæssige modstandskraft og holdbarhed
    iii. forretningskontinuitet og operationelle modstandskraft
    iv. operationelle risici, herunder adfærdsmæssige, IKT-mæssige og juridiske risici
    v. omdømmemæssige risici.

b. potentielle konsekvenser af cloud-outsourcingaftalen for selskabets evne til at:
    i. identificere, overvåge og styre alle relevante risici
    ii. overholde alle lovgivningsmæssige og administrative krav
    iii. foretage passende revisioner vedrørende den outsourcede operationelle funktion eller aktivitet.

c. selskabets (og/eller i givet fald koncernens) samlede eksponering overfor den samme cloududbyder og den potentielle samlede indvirkning af outsourcingaftaler inden for samme forretningsområde

d. størrelsen og kompleksiteten af de af selskabets forretningsområder, der berøres af cloud-outsourcingaftalen

e. muligheden for om nødvendigt og hvis ønsket at overføre den foreslåede cloudydelse til en anden cloududbyder, eller reintegrere tjenesteydelserne ("substituerbarhed")

f. beskyttelsen af personoplysninger og ikke-personoplysninger, og de potentielle konsekvenser for selskabet, forsikringstagerne eller andre relevante personer af et brud på fortroligheden eller af manglende sikring af datatilgængelighed og -integritet, bl.a. baseret på forordning (EU) 2016/679[7]. Selskabet bør navnlig

[7] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

tage hensyn til oplysninger, der er forretningshemmeligheder og/eller følsomme (f.eks. forsikringstageres sundhedsoplysninger).

Retningslinje 8 – risikovurdering af cloudoutsourcing

30. Som hovedregel bør selskabet vælge en tilgang, der står i rimeligt forhold til arten, omfanget og kompleksiteten af de iboende risici ved de tjenester, der outsources til cloududbydere. Det indebærer at vurdere de potentielle konsekvenser af enhver cloudoutsourcing, navnlig i forhold til dets operationelle og omdømmemæssige risici.

31. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter til cloududbydere bør selskabet:

a. tage hensyn til de forventede fordele og omkostninger ved den påtænkte cloud-outsourcingaftale, herunder afveje eventuelle væsentlige risici, der kan mindskes eller forvaltes bedre i forhold til væsentlige risici, der kan opstå som følge af den påtænkte cloud-outsourcingaftale

b. når det er relevant og hensigtsmæssigt, vurdere de risici, herunder vedrørende juridiske forhold, IKT, regeloverholdelse og omdømme, samt begrænsninger i tilsynet, som følger af:

   i. den valgte cloudtjeneste og de påtænkte implementeringsmodeller (dvs. offentlig/privat/hybrid/fælles)

   ii. migrationen og/eller implementeringen

   iii. de aktiviteter og relaterede data og systemer, der overvejes outsourcet (eller er outsourcet), deres følsomhed og de sikkerhedsforanstaltninger, de kræver

   iv. den politiske stabilitet og sikkerhedssituationen i de lande (i eller uden for EU), hvor de outsourcede tjenesteydelser leveres fra eller kan blive leveret fra, og hvor dataene vil blive lagret eller kan forventes at blive det. Ved vurderingen bør følgende tages i betragtning:

      1. gældende lovgivning, herunder lovgivning om databeskyttelse

      2. gældende bestemmelser om retshåndhævelse

      3. bestemmelser i insolvenslovgivningen, som finder anvendelse ved en tjenesteudbyders konkurs, og eventuelle begrænsninger, der vil opstå hvad angår presserende genopretning af selskabets data

   v. videreoutsourcing, herunder de ekstra risici, der kan opstå, hvis underkontrahenten er hjemmehørende i et tredjeland eller et andet land end cloududbyderens, og risikoen for, at lange, komplekse kæder af videreoutsourcing forringer selskabets mulighed for at føre tilsyn med sine kritiske eller vigtige operationelle funktioner eller aktiviteter, og tilsynsmyndighedernes mulighed for effektivt at overvåge dem

   vi. selskabets samlede koncentrationsrisiko overfor den samme cloududbyder, herunder outsourcing til en cloududbyder, der ikke let kan substitueres, eller flere outsourcingaftaler med samme cloududbyder. Ved vurderingen af koncentrationsrisikoen bør

selskabet (og/eller i givet fald koncernen) medregne alle sine cloud-outsourcingaftaler med den pågældende cloududbyder.

32. Risikovurderingen bør foretages, inden der indgås en cloud-outsourcingaftale. Får selskabet kendskab til væsentlige mangler og/eller væsentlige ændringer i de leverede tjenester eller i cloududbyderens situation, bør risikovurderingen straks gennemgås eller gentages. Ved fornyelse af en cloud-outsourcingaftale hvad angår dens indhold og anvendelsesområde (f.eks. udvidelse af anvendelsesområdet eller inddragelse i anvendelsesområdet af kritiske eller vigtige operationelle funktioner, som ikke tidligere har indgået), bør risikovurderingen gentages.

Retningslinje 9 – due diligence vedrørende cloududbyder

33. Selskabet bør i sin udvælgelses- og vurderingsproces sikre sig, at cloududbyderen er egnet efter kriterierne i selskabets skriftlige outsourcingpolitik.

34. Forud for outsourcing af en operationel funktion eller aktivitet bør der foretages due diligence i forhold til cloududbyderen. Hvis selskabet indgår endnu en aftale med en cloududbyder, der allerede er vurderet, bør selskabet ved en risikobaseret tilgang afgøre, om der er behov for endnu en due diligence-gennemgang. Får selskabet kendskab til væsentlige mangler og/eller væsentlige ændringer i de leverede tjenester eller i cloududbyderens situation, bør den foretagne due diligence straks genbesøges eller gentages.

35. Ved cloudoutsourcing af kritiske eller vigtige operationelle funktioner bør due diligence omfatte en evaluering af cloududbyderens egnethed (f.eks. færdigheder, infrastruktur, økonomisk situation, virksomhedsmæssig og regulatorisk status). Hvor det er relevant, kan selskabet støtte den foretagne due diligence-gennemgang med dokumentation, certificeringer efter internationale standarder, revisionsrapporter fra anerkendte tredjeparter eller interne revisionsrapporter.

Retningslinje 10 – kontraktvilkår

36. Rettigheder og forpligtelser for henholdsvis selskabet og cloududbyderen bør fremstå klare og fastlægges i en skriftlig aftale.

37. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter til en cloududbyder og med forbehold for kravene i artikel 274 i den delegerede forordning bør den skriftlige aftale mellem selskabet og cloududbyderen indeholde:

a. en klar beskrivelse af den outsourcede funktion, som skal leveres (cloudtjenester, herunder arten af supporttjenester)

b. start- og slutdato for aftalen, hvor det er relevant, og opsigelsesfrister for cloududbyderen og for selskabet

c. det værneting og den lovgivning, kontrakten er undergivet

d. parternes finansielle forpligtelser

e. hvorvidt videreoutsourcing af en kritisk eller vigtig operationel funktion eller aktivitet (eller væsentlige dele heraf) er tilladt, og, i så fald, de betingelser, som den væsentlige videreoutsourcing er underlagt (jf. retningslinje 13)

f. stedet eller stederne (dvs. de regioner eller lande), hvor relevante data vil blive opbevaret og behandlet (datacentrenes placering), og de betingelser, der skal opfyldes, herunder et krav om at underrette selskabet, hvis tjenesteudbyderen påtænker at ændre stedet eller stederne

g. bestemmelser om adgangsmuligheder, tilgængelighed, integritet, fortrolighed og sikkerhed i forhold til relevante data under hensyntagen til specifikationerne i retningslinje 12

h. selskabets ret til regelmæssigt at føre tilsyn med cloududbyderens udførelse af aktiviteter

i. de aftalte serviceniveauer, som bør omfatte præcise kvantitative og kvalitative præstationsmål for at give mulighed for rettidig overvågning, så der i tilfælde af manglende overholdelse af aftalte serviceniveauer kan træffes passende korrigerende foranstaltninger uden unødig forsinkelse

j. cloududbyderens forpligtelser til at rapportere til selskabet, herunder, hvis det er hensigtsmæssigt, forelægge rapporter, som er relevante for selskabets sikkerhedsfunktion og nøglefunktioner, f.eks. rapporter fra cloududbyderens interne revisionsfunktion

k. om cloududbyderen er forpligtet til at tegne forsikring mod visse risici, og, i så fald, størrelsen af den krævede forsikringsdækning

l. krav til at gennemføre og teste beredskabsplaner for forretningskontinuitet

m. krav om, at cloududbyderen skal give selskabet, dets tilsynsmyndigheder og enhver anden person, der udpeges af selskabet eller tilsynsmyndighederne, følgende:

    i. fuld adgang til alle relevante forretningslokaler (hovedkontorer og operationelle centre), herunder alle relevante enheder, systemer, netværk, oplysninger og data, der anvendes til at udføre den outsourcede funktion, herunder de tilknyttede finansielle oplysninger, det tilknyttede personale og cloududbyderens eksterne revisorer ("adgangsrettigheder")

    ii. ubegrænset ret til inspektion og revision relateret til cloud-outsourcingaftalen ("revisionsrettigheder") for at give mulighed for at overvåge cloud-outsourcingaftalen og sikre overholdelsen af alle gældende myndighedskrav og kontraktlige krav

n. bestemmelser, der sikrer, at data, der ejes af selskabet, straks kan tilgås i tilfælde af cloududbyderens insolvens eller ophør af forretningsaktiviteter.

Retningslinje 11 — adgangs- og revisionsrettigheder

38. Aftalen om cloudoutsourcing bør ikke begrænse selskabets faktiske udøvelse af adgangs- og revisionsrettigheder eller kontrolmuligheder for cloudtjenester med henblik på at opfylde sine lovbestemte forpligtelser.

39. Selskabet bør anvende en risikobaseret tilgang i udøvelsen af sine adgangs- og revisionsrettigheder, fastlæggelsen af revisionshyppigheden og de områder og tjenester, der skal revideres, jf. afsnit 8 i EIOPA's "Retningslinjer for ledelsessystem".

40. Ved fastlæggelsen af hyppigheden og omfanget af sin udøvelse af adgangs- eller revisionsrettigheder bør selskabet tage hensyn til, om cloud-outsourcingen vedrører en kritisk eller vigtig operationel funktion eller aktivitet, risicienes art og størrelse, og cloud-outsourcingaftalernes indvirkning på selskabet.

41. Hvis udøvelsen af selskabets adgangs- eller revisionsrettigheder eller anvendelsen af visse revisionsteknikker medfører en risiko for miljøet hos cloududbyderen og/eller en anden cloududbyders kunde (f.eks. indvirkning på serviceniveau, datatilgængelighed, fortrolighedsaspekter), bør selskabet og

cloududbyderen aftale alternative måder, hvorpå der kan gives et tilsvarende niveau af sikkerhed og service til selskabet (f.eks. anvendelse af specifikke kontroller, der testes i henhold til en særlig rapport/certificering, som cloududbyderen udarbejder).

42. Uden at det berører selskabernes endelige ansvar for de aktiviteter, der udføres af deres cloududbydere, kan selskaberne anvende følgende for at udnytte revisionsressourcerne mere effektivt og mindske den organisatoriske byrde for cloududbyderen og dennes kunder:

a. tredjepartscertificeringer og -revisionsrapporter eller interne revisionsrapporter, som cloududbyderen stiller til rådighed

b. poolede revisioner (dvs. revisioner foretaget sammen med andre kunder hos samme cloududbyder) eller poolede revisioner, som udføres af en tredjepart, de har udpeget.

43. Til cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter bør selskaberne kun benytte metoden i punkt 42 a, såfremt de:

a. sikrer, at certificeringen eller revisionsrapporten omfatter de systemer (dvs. processer, applikationer, infrastruktur, datacentre mv.) og kontroller, som selskabet har fastlagt, og vurderer efterlevelsen af relevante myndighedskrav

b. regelmæssigt foretager en indgående vurdering af nye certificeringer eller revisionsrapporter og kontrollerer, at certificeringer og rapporter ikke er forældede

c. sikrer, at centrale systemer og kontroller indgår i fremtidige versioner af certificeringen eller revisionsrapporten

d. finder certificerings- eller revisionsvirksomheden tilfredsstillende egnet (f.eks. hvad angår rotation i certificerings- eller revisionsvirksomheden, kvalifikationer, ekspertise, fornyet udarbejdelse/verificering af dokumentationen i de underliggende revisionsakter)

e. finder, at de udstedte certifikater og foretagne revisioner er tilfredsstillende i henhold til anerkendte standarder, og at de indbefatter en test af den operationelle effektivitet af de vigtigste anvendte kontroller

f. har kontraktlig ret til at anmode om, at anvendelsesområdet for certificeringer eller revisionsrapporter udvides til andre relevante systemer og kontroller, idet sådanne anmodninger om ændring af anvendelsesområdet bør have et rimeligt antal og en rimelig hyppighed og skal være berettigede ud fra et risikostyringsperspektiv

g. bibeholder den kontraktlige ret til at foretage individuelle revisioner på stedet efter eget skøn vedrørende cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter. Denne ret bør udøves, når der er særlige behov, som ikke kan opfyldes gennem andre former for interaktion med cloududbyderen.

44. For outsourcing af kritiske eller vigtige operationelle funktioner til cloududbydere bør selskabet vurdere, om tredjepartscertificeringer og -rapporter som omhandlet i punkt 42 a er egnede og tilstrækkelige til at opfylde selskabets lovbundne forpligtelser, og på baggrund af en risikobaseret tilgang bør selskabet over tid ikke udelukkende forlade sig på sådanne rapporter og certifikater.

45. Før der aflægges et planlagt besøg på stedet, bør den part, der udøver sin adgangsret (selskab, revisor eller en tredjepart, der handler på vegne af selskabet eller selskaberne), give forhåndsunderretning med en rimelig frist, medmindre tidlig forhåndsunderretning ikke har været mulig som følge af en nød- eller krisesituation.

En sådan underretning bør omfatte stedet for og formålet med besøget og det personale, der deltager i besøget.

46. I betragtning af, at cloudløsninger har et højt teknisk kompleksitetsniveau, bør selskabet efterprøve, om de medarbejdere, der udfører revisionen – hvad enten det er interne revisorer eller den pulje af revisorer, der handler på dets vegne, eller de revisorer, som cloududbyderen udpeger, eller, i givet fald, det personale, der gennemgår tredjepartscertificeringen eller tjenesteudbyderens revisionsrapporter – har erhvervet tilstrækkeligt med færdigheder og viden til at kunne udføre de relevante revisioner og/eller vurderinger.

Retningslinje 12 – data- og systemsikkerhed

47. Selskabet bør sikre, at cloududbyderne overholder europæiske og nationale bestemmelser samt passende standarder for IKT-sikkerhed.

48. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter til cloududbydere bør selskabet desuden i aftalen om outsourcing fastlægge specifikke krav til informationssikkerhed, og regelmæssigt overvåge overholdelsen heraf.

49. Ved outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter til cloududbydere bør selskabet – med henblik på punkt 48, ud fra en risikobaseret tilgang og under hensyntagen til sine egne og cloududbyderens ansvarsområder – gøre følgende:

a. aftale klare roller og ansvarsområder for cloududbyderen og selskabet i forbindelse med de operationelle funktioner eller aktiviteter, der berøres af cloudoutsourcingen, og som bør være klart opdelt

b. definere og fastlægge et passende niveau for beskyttelsen af fortrolige data, kontinuiteten af de outsourcede aktiviteter, og integriteten og sporbarheden af data og systemer i forbindelse med den tilsigtede cloudoutsourcing.

c. om nødvendigt overveje specifikke foranstaltninger for data i overførsel, data i hukommelsen og data i hvile, f.eks. anvendelse af krypteringsteknologier i kombination med tilbørlig styring af krypteringsnøgler

d. overveje mekanismerne til integration af cloudtjenesterne med selskabets systemer, f.eks. programmeringsgrænseflader for applikationer, og en forsvarlig procedure til bruger- og adgangsstyring

e. kontraktligt sikre, at den tilgængelige netværkskapacitet og den forventede kapacitet opfylder strenge krav til kontinuitet, hvor dette er relevant og muligt

f. definere og fastlægge passende krav til kontinuitet, der sikrer et tilstrækkeligt niveau på hvert niveau af teknologikæden, hvor dette er relevant

g. have indført en forsvarlig, veldokumenteret procedure for håndtering af hændelser, herunder de forskellige ansvarsområder, f.eks. ved at fastlægge en model for samarbejde i tilfælde af faktiske eller formodede hændelser

h. anvende en risikobaseret tilgang til stedet (stederne) (dvs. land eller region) til datalagring og -behandling og til informationssikkerhedshensyn

i. overvåge opfyldelsen af kravene vedrørende effektiviteten og tilstrækkeligheden af de kontrolmekanismer, som er gennemført af cloududbyderen, og som vil kunne afbøde de risici, der er forbundet med de ydede tjenester.

Retningslinje 13 – videreoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter

50. Hvis det er tilladt at videreoutsource kritiske eller vigtige operationelle funktioner (eller en del heraf), bør aftalen om cloudoutsourcing mellem selskabet og cloududbyderen:

a. angive alle typer af aktiviteter, der er udelukket fra eventuel videreoutsourcing

b. angive de betingelser, der skal overholdes ved videreoutsourcing (f.eks. at den, der videreoutsources til, også opfylder cloududbyderens relevante forpligtelser). Disse forpligtelser omfatter revisions- og adgangsrettigheder og data- og systemsikkerhed

c. angive, at cloududbyderen bibeholder fuldt ansvar og fuld tilsynspligt vedrørende de tjenester, der videreoutsources

d. indeholde en forpligtelse for cloududbyderen til at oplyse selskabet om alle påtænkte væsentlige ændringer hos underkontrahenter eller af videreoutsourcede tjenesteydelser, som kan tænkes at ville påvirke tjenesteudbyderens evne til at opfylde sine forpligtelser i henhold til outsourcingaftalen. Fristen for notifikation af sådanne ændringer skal gøre det muligt for selskabet som minimum at udføre en risikovurdering af konsekvenserne af de påtænkte ændringer inden der foretages en faktisk ændring hos den, der videreoutsources til, eller af de videreoutsourcede tjenesteydelser

e. sikre sig, at hvis en cloududbyder påtænker ændringer i forhold til den, der videreoutsources til, eller ændringer i forhold til de videreoutsourcede serviceydelser, og hvis dette vil have ugunstig virkning på risikovurderingen for de aftalte serviceydelser, har selskabet ret til at modsætte sig sådanne ændringer og/eller at bringe kontrakten til ophør eller udtræde af den.

Retningslinje 14 – overvågning og tilsyn i forbindelse med cloud-outsourcingaftaler

51. Selskabet bør ud fra en risikobaseret tilgang regelmæssigt overvåge sine cloududbyderes udførelse af aktiviteter, sikkerhedsforanstaltningerne og overholdelsen af det aftalte serviceniveau. Hovedvægten bør lægges på cloudoutsourcing af kritiske og vigtige operationelle funktioner.

52. Til dette formål bør selskabet etablere overvågnings- og tilsynsmekanismer som – når det er muligt og hensigtsmæssigt – tager hensyn til tilstedeværelsen af videreoutsourcing af kritiske eller vigtige operationelle funktioner eller en del deraf.

53. Administrations-, ledelses- eller tilsynsorganet (AMSB) bør regelmæssigt holdes orienteret om konstaterede risici i forbindelse med cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter.

54. For at sikre tilstrækkelig overvågning af og tilsyn med deres cloud-outsourcingaftaler bør selskaberne anvende de fornødne ressourcer med tilstrækkelige færdigheder og viden til at overvåge de tjenesteydelser, der outsources til "skyen". Det af selskabets personale, der har ansvar for disse aktiviteter, bør have viden både på IKT- og forretningsområdet i det omfang, der skønnes nødvendigt.

Retningslinje 15 – opsigelsesrettigheder og exit-strategier

55. Ved cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter bør aftalen om cloudoutsourcing indeholde en klausul med en klart defineret exit-strategi, der sikrer, at selskabet om nødvendigt kan opsige aftalen. Det bør være muligt at opsige kontrakten, uden at det er til skade for kontinuiteten og kvaliteten af selskabets tjenesteydelser til forsikringstagerne. For at sikre dette bør selskabet:

a. udarbejde exit-planer, der er udførlige, servicebaserede, veldokumenterede og tilstrækkeligt testet (f.eks. ved at foretage en analyse af de potentielle omkostninger, konsekvenser og ressourcemæssige og tidsmæssige implikationer af de forskellige potentielle exit-muligheder)

b. identificere alternative løsninger og udarbejde egnede og gennemførlige overgangsplaner, der sætter selskabet i stand til at fjerne eksisterende aktiviteter og data fra cloududbyderen og overføre dem til alternative tjenesteudbydere eller tilbage til selskabet. Disse løsninger bør fastlægges ud fra de udfordringer, der kan opstå som følge af dataenes placering, og med anvendelse af de nødvendige foranstaltninger til at sikre forretningskontinuitet i overgangsfasen

c. sikre, at cloududbyderen yder selskabet tilstrækkelig support i forbindelse med overførsel af de outsourcede data, systemer eller applikationer til en anden tjenesteudbyder eller direkte til selskabet

d. aftale med cloududbyderen, at dens data, når de er ført tilbage til selskabet, vil blive slettet fuldstændigt og sikkert af cloududbyderen i alle regioner.

56. Ved udarbejdelsen af exit-strategier bør selskabet tage følgende i betragtning:

a. fastlægge målsætningerne for exit-strategien

b. fastlægge de udløsende hændelser der kan aktivere exit-strategien (f.eks. at centrale risikoindikatorer angiver et uacceptabelt serviceniveau)

c. udføre en analyse af konsekvenserne for selskabet, der står i rimeligt forhold til de outsourcede aktiviteter, for at fastlægge, hvilke menneskelige og materielle ressourcer der vil være påkrævede for at gennemføre exit-planen, og hvor lang tid dette vil tage

d. fordele roller og ansvarsområder i styringen af exit-planerne og overgangsaktiviteterne

e. fastlægge succeskriterier for overgangen.

Retningslinje 16 – myndighedernes tilsyn med cloud-outsourcingaftaler

57. Tilsynsmyndighederne bør som led i deres tilsynsproces foretage en analyse af indvirkningerne af selskabernes cloud-outsourcingaftaler. Analysen af indvirkningerne bør navnlig fokusere på aftaler i forbindelse med outsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter.

58. Tilsynsmyndighederne bør overveje følgende risici i forbindelse med tilsynet med selskabernes cloud-outsourcingaftaler:

a. IKT-risici

b. andre operationelle risici (herunder risici vedrørende juridiske forhold og regelefterlevelse, outsourcing og tredjepartsrisikostyring)

c. omdømmemæssige risici

d. koncentrationsrisiko, herunder på lande- og sektorniveau.

59. Tilsynsmyndighederne bør i deres vurdering inddrage følgende aspekter baseret på en risikobaseret tilgang:

a. hensigtsmæssigheden og effektiviteten af selskabets styringsmæssige og operationelle processer i forbindelse med godkendelse, gennemførelse, overvågning, forvaltning og fornyelse af cloud-outsourcingaftaler

b. om selskabet har de fornødne ressourcer med tilstrækkelige færdigheder og viden til at kunne overvåge tjenester, der outsources til skyen

c. om selskabet fastlægger og styrer alle risici, der er fremhævet i disse retningslinjer.

60. For koncerner bør den tilsynsførende for koncernen sikre, at konsekvenserne af cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter afspejles i risikovurderingen for koncernen under hensyntagen til kravene i punkt 58-59 og koncernens individuelle ledelsesmæssige og operationelle karakteristika.

61. Hvis cloudoutsourcing af kritiske eller vigtige operationelle funktioner eller aktiviteter involverer mere end én virksomhed i forskellige medlemsstater og styres centralt af moderselskabet eller et koncerndatterselskab (f.eks. selskabets eller koncernens IKT-leverandør), bør den tilsynsførende for koncernen og/eller de relevante tilsynsmyndigheder for de virksomheder, der er involveret i cloudoutsourcingen, i tilsynskollegiet drøfte cloudoutsourcingens konsekvenser for koncernens risikoprofil, hvis dette er hensigtsmæssigt.

62. Konstateres der betænkeligheder, som fører til den konklusion, at selskabet ikke længere anvender robuste ledelsesmæssige foranstaltninger eller ikke opfylder lovgivningskravene, bør tilsynsmyndighederne træffe passende foranstaltninger, f.eks. at kræve, at selskabet forbedrer de ledelsesmæssige foranstaltninger, at det begrænser eller indskrænker omfanget af de outsourcede funktioner, eller at det udtræder af en eller flere outsourcingaftaler. Idet der navnlig tages hensyn til behovet for at sikre kontinuiteten af selskabets drift, kan der stilles krav om annullering af kontrakter, såfremt tilsynet og håndhævelse af lovgivningskravene ikke kan sikres gennem andre foranstaltninger.

Bestemmelser om efterlevelse og indberetning

63. Dette dokument indeholder retningslinjer udstedt i henhold til artikel 16 i forordning (EU) nr. 1094/2010. I henhold til artikel 16, stk. 3, i nævnte forordning skal de kompetente myndigheder og finansielle institutioner bestræbe sig mest muligt på at efterleve retningslinjer og henstillinger.

64. Kompetente myndigheder, der efterlever eller agter at efterleve disse retningslinjer, bør på passende måde indarbejde dem i deres lovgivnings- eller tilsynsramme.

65. De kompetente myndigheder skal over for EIOPA bekræfte, om de efterlever eller agter at efterleve disse retningslinjer, og i modsat fald angive begrundelsen for den manglende efterlevelse inden for to måneder efter udstedelsen af de oversatte versioner.

66. Hvis de kompetente myndigheder ikke har reageret inden udløbet af denne frist, vil det blive betragtet som manglende efterlevelse af indberetningskravet, hvilket vil blive offentliggjort.

Afsluttende bestemmelse om revision

67. Disse retningslinjer vil blive revideret af EIOPA.