EIOPA-BoS-20-002

Riktlinjer om uppdragsavtal med molntjänstleverantörer

Innehållsförteckning

Inledning

1. I enlighet med artikel 16 i förordning (EU) nr 1094/2010[1] utfärdar Eiopa riktlinjer som ger försäkrings- och återförsäkringsföretag vägledning om hur bestämmelserna om uppdragsavtal i direktiv 2009/138/EG[2] (*Solvens II*) och i kommissionens delegerade förordning (EU) 2015/35[3] (*den delegerade förordningen*) ska tillämpas för uppdragsavtal med molntjänstleverantörer.
2. Dessa riktlinjer utgår från artiklarna 13.28, 38 och 49 i Solvens II och artikel 274 i den delegerade förordningen. Dessutom bygger dessa riktlinjer på den vägledning som ges i Eiopas riktlinjer för företagsstyrningssystem (EIOPA-BoS-14/253).
3. Dessa riktlinjer vänder sig till behöriga myndigheter och syftar till att ge vägledning om hur försäkrings- och återförsäkringsföretag (nedan kallade ”företag”) bör tillämpa de krav på uppdragsavtal som läggs fram i ovanstående rättsakter när det gäller utkontraktering till molntjänstleverantörer.
4. Riktlinjerna gäller både enskilda företag och i tillämpliga delar grupper[4].

   Enheter som är föremål för andra sektorskrav, och som ingår i en grupp, omfattas inte av dessa riktlinjer på företagsnivå eftersom de måste följa de sektorspecifika kraven samt den relevanta vägledning som utfärdas av Europeiska värdepappers- och marknadsmyndigheten samt Europeiska bankmyndigheten.
5. Vid uppdragsavtal inom gruppen och avtal om underentreprenad med molntjänstleverantörer bör dessa riktlinjer tillämpas tillsammans med bestämmelserna i Eiopas riktlinjer för företagsstyrningssystem avseende uppdragsavtal inom gruppen.
6. Företag och behöriga myndigheter bör beakta proportionalitetsprincipen[5] och hur kritisk eller viktig den tjänst är som läggs ut på molntjänstleverantörer, när de efterlever eller övervakar efterlevnad av dessa riktlinjer. Proportionalitetsprincipen bör säkerställa att styrformer, inbegripet sådana som avser uppdragsavtal med molntjänstleverantörer, är proportionerliga i förhållande till de underliggande riskernas art, omfattning och komplexitet.
7. Dessa riktlinjer bör gälla tillsammans med och utan att påverka Eiopas riktlinjer för företagsstyrningssystem samt de lagstadgade skyldigheter som förtecknas i punkt 1.

Definitioner

8. Termer som inte definieras i dessa riktlinjer har den betydelse som anges i de rättsakter som det hänvisas till i inledningen.
9. I riktlinjerna gäller dessutom följande definitioner:

Tjänsteleverantör	En enhet från tredje part som utför en process, tjänst eller verksamhet, eller delar därav, inom ramen för en överenskommelse om uppdragsavtal.

[1] Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48).

[2] Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

[3] Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 12, 17.1.2015, s. 1).

[4] Artikel 212.1 i Solvens II.

[5] Artikel 29.3 i Solvens II.

Molntjänstleverantör	En tjänsteleverantör enligt definitionen ovan som ansvarar för att tillhandahålla molntjänster inom ramen för ett uppdragsavtal.
Molntjänster	Tjänster som tillhandahålls med hjälp av molnbaserade datortjänster, dvs. en modell som möjliggör en allmän, lämplig nätverksåtkomst på begäran till en gemensam samling konfigurerbara datorresurser (t.ex. nätverk, servrar, lagring, applikationer och tjänster) som snabbt kan tillhandahållas och överlåtas med minimala driftsinsatser eller interaktion med tjänsteleverantören.
Offentligt moln	Molninfrastruktur som är tillgänglig för öppen användning av allmänheten.
Privat moln	Molninfrastruktur som är tillgänglig för exklusiv användning av ett enda företag.
Gemenskapsmoln	Molninfrastruktur som är tillgänglig för exklusiv användning av en särskild företagsgemenskap, till exempel flera företag inom en och samma grupp.
Hybridmoln	Molninfrastruktur som består av två eller fler separata molninfrastrukturer.

Tillämpningsdatum

10. Dessa riktlinjer gäller från och med den 1 januari 2021 för alla uppdragsavtal om molntjänster som ingås eller ändras på eller efter detta datum.

11. Företag bör se över och ändra befintliga arrangemang för uppdragsavtal om molntjänster som avser kritiska eller viktiga operativa funktioner eller verksamheter i syfte att säkerställa efterlevnad av dessa riktlinjer senast den 31 december 2022.

12. Om granskningen av uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter inte är färdig senast den 31 december 2022 ska företaget informera sin tillsynsmyndighet[6] om detta faktum, inbegripet åtgärder som planerats för att fullgöra granskningen eller den möjliga utträdesstrategin. Tillsynsmyndigheten kan komma överens med företaget om en förlängd tidsfrist för att slutföra översynen, om så är lämpligt.

13. Uppdateringen (vid behov) av företagets policyer och interna processer bör vara klar den 1 januari 2021, medan dokumentationskraven för överenskommelser om uppdragsavtal om molntjänster av kritiska eller viktiga operativa funktioner eller verksamheter bör genomföras senast den 31 december 2022.

[6] Artikel 13.10 i Solvens II.

Riktlinje 1 – Molntjänster och uppdragsavtal

14. Företaget bör fastställa om en överenskommelse med en molntjänstleverantör omfattas av definitionen av uppdragsavtal i enlighet med Solvens II. Inom ramen för bedömningen bör följande beaktas:

a. Huruvida den operativa funktionen eller verksamheten (eller en del därav) som omfattas av uppdragsavtal är återkommande eller kontinuerlig.

b. Huruvida den här operativa funktionen eller verksamheten (eller en del därav) vanligen skulle omfattas av sådana operativa funktioner eller verksamheter som skulle eller skulle kunna utföras av företaget inom ramen för dess normala affärsverksamhet, även om företaget inte har utfört denna operativa funktion eller verksamhet tidigare.

15. Om en överenskommelse med en tjänsteleverantör omfattar flera operativa funktioner eller verksamheter bör företaget beakta alla aspekter av överenskommelsen i sin bedömning.

16. I fall då företaget ingår uppdragsavtal för operativa funktioner eller verksamheter med tjänsteleverantörer som inte är molntjänstleverantörer, men till stor del är beroende av molninfrastrukturer för att tillhandahålla sina tjänster (till exempel om molntjänstleverantören ingår i en underentreprenörskedja), omfattas överenskommelsen om detta uppdragsavtal av dessa riktlinjer.

Riktlinje 2 – Allmänna principer för styrning av uppdragsavtal om molntjänster

17. Utan att det påverkar artikel 274.3 i den delegerade förordningen bör företagets förvaltnings-, lednings- eller tillsynsorgan säkerställa att ett beslut om att ingå uppdragsavtal om kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer fattas på grundval av en noggrann riskbedömning som omfattar alla relevanta risker som överenskommelsen kan medföra, exempelvis avseende informations- och kommunikationsteknik (IKT), affärskontinuitet, lagstiftning och efterlevnad, koncentration samt övriga operativa risker och risker som rör datamigrering och/eller genomförandefasen, om så är tillämpligt.

18. Om kritiska eller viktiga operativa funktioner eller verksamheter läggs ut på molntjänstleverantörer bör företaget i tillämpliga fall låta ändringarna i dess riskprofil på grund av överenskommelserna om uppdragsavtal om molntjänster återspeglas i den egna risk- och solvensbedömningen.

19. Användningen av molntjänster bör ske i enlighet med företagets strategier (till exempel IKT-strategi, informationssäkerhetsstrategi, strategi för hantering av operativa risker) samt interna policyer och processer och dessa bör vid behov uppdateras.

Riktlinje 3 – Uppdatering av den skriftliga policyn om uppdragsavtal

20. Vid uppdragsavtal med molntjänstleverantörer bör företaget uppdatera den skriftliga policyn om uppdragsavtal (till exempel genom att se över den, lägga till en separat bilaga eller ta fram nya särskilda policyer) samt övriga relevanta interna policyer (till exempel informationssäkerhet), med beaktande av särdrag som gäller uppdragsavtal om molntjänster på åtminstone följande områden:

a. Roller och ansvarsområden för företagets berörda funktioner, i synnerhet förvaltnings-, lednings- eller tillsynsorgan, och funktionerna som ansvarar för IKT, informationssäkerhet, efterlevnad, riskhantering och internrevision.

b. Processerna och rapporteringsförfarandena som krävs för godkännande, genomförande, övervakning, förvaltning och förnyelse, där så är tillämpligt, av överenskommelser om uppdragsavtal om molntjänster som avser kritiska eller viktiga operativa funktioner eller verksamheter.

c. Översyn av molntjänsterna i proportion till art, omfattning och komplexitet för de tillhandahållna tjänsternas risker, inbegripet i) riskbedömning av överenskommelser om uppdragsavtal om molntjänster och företagsbesiktning av molntjänstleverantörer, inklusive riskbedömningens frekvens, ii) övervaknings- och förvaltningskontroller (till exempel verifiering av servicenivåavtalet) samt iii) säkerhetsstandarder och -kontroller.

d. Avseende uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter bör en hänvisning göras till de avtalsenliga kraven i enlighet med riktlinje 10.

e. Dokumentationskrav och skriftligt meddelande till tillsynsmyndigheten om uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter.

f. Avseende varje enskild överenskommelse om uppdragsavtal om molntjänster som omfattar kritiska eller viktiga operativa funktioner eller verksamheter krävs en dokumenterad och i tillämpliga fall tillräckligt testad utträdesstrategi som är proportionerlig till art, omfattning och komplexitet för de tillhandahållna tjänsternas risker. Utträdesstrategin kan inbegripa ett antal förfaranden för uppsägning, inklusive men inte nödvändigtvis begränsat till, att avsluta, återintegrera eller överföra tjänsterna som omfattas av överenskommelsen om uppdragsavtal om molntjänster.

Riktlinje 4 – Skriftligt meddelande till tillsynsmyndigheten

21. Kraven på skriftligt meddelande som fastställs i artikel 49.3 i Solvens II och specificeras ytterligare i Eiopas riktlinjer för företagsstyrningssystem gäller alla uppdragsavtal för kritiska eller viktiga operativa funktioner och verksamheter med molntjänstleverantörer. Om en operativ funktion eller verksamhet som omfattas av uppdragsavtal tidigare klassades som ej kritisk eller ej viktig blir kritisk eller viktig bör företaget meddela tillsynsmyndigheten.

22. Företagets skriftliga meddelande bör i enlighet med proportionalitetsprincipen åtminstone innefatta följande information:

a. En kort beskrivning av den operativa funktion eller verksamhet som omfattas av uppdragsavtal.

b. Startdatum och, efter vad som är tillämpligt, datum för nästa kontraktsförnyelse, slutdatum och/eller anmälningsperioder för molntjänstleverantören och för företaget.

c. Den lagstiftning som gäller för överenskommelsen om uppdragsavtal om molntjänster.

d. Molntjänstleverantörens namn, organisationsnumret, identifieringskoden för juridisk person (LEI) (när sådan finns), den registrerade adressen och andra relevanta kontaktuppgifter, samt namnet på leverantörens moderföretag (om sådant finns), och vid grupper huruvida molntjänstleverantören ingår i gruppen.

e. Molntjänsterna och distribueringsmodellerna (dvs. offentligt moln/privat moln/hybridmoln/gemenskapsmoln) och den särskilda karaktären på

uppgifterna som ska hållas och platserna (dvs. länder eller regioner) där sådana uppgifter kommer att lagras.

f. En kort sammanfattning av anledningarna till att den operativa funktion eller verksamhet som omfattas av uppdragsavtal anses vara kritisk eller viktig.

g. Datumet för den senaste bedömningen av om den operativa funktion eller verksamhet som omfattas av uppdragsavtal är kritisk eller viktig.

Riktlinje 5 – Dokumentationskrav

23. Som en del av sitt styrnings- och riskhanteringssystem bör företaget föra ett register över sina överenskommelser om uppdragsavtal om molntjänster, till exempel genom ett särskilt register som uppdateras löpande. Företaget bör också föra ett register över avslutade överenskommelser om uppdragsavtal om molntjänster under en lämplig lagringsperiod i enlighet med nationell lagstiftning.

24. Vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter bör företaget registrera följande information:

a. Informationen som ska meddelas tillsynsmyndigheten i enlighet med riktlinje 4.

b. Om grupper förekommer: de försäkrings- eller återförsäkringsföretag och andra företag inom ramen för den konsoliderade tillsynen som använder molntjänsterna.

c. Datumet för den senaste riskbedömningen och en kort sammanfattning av huvudresultaten.

d. Det enskilda eller beslutsfattande organet (till exempel förvaltnings-, ledningseller tillsynsorganet) i företaget som godkände överenskommelsen om uppdragsavtal om molntjänster.

e. Datumen för de senaste och närmast planerade revisionerna, i tillämpliga fall.

f. Namnen på eventuella underentreprenörer som väsentliga delar av en kritisk eller viktig operativ funktion eller verksamhet läggs ut på underentreprenad till, däribland de länder där underentreprenörerna är registrerade, var tjänsten kommer att utföras och i tillämpliga fall de platser (dvs. länder eller regioner) där uppgifterna kommer att lagras.

g. Ett resultat av bedömningen av molntjänstleverantörens utbytbarhet (till exempel lätt, svår eller omöjlig).

h. Huruvida den kritiska eller viktiga operativa funktionen eller verksamheten som omfattas av uppdragsavtal stöder affärsverksamheter som är tidsmässigt kritiska.

i. De beräknade årliga budgetkostnaderna.

j. Huruvida företaget har en utträdesstrategi i händelse av uppsägning av avtalet av endera parten eller störningar i molntjänstleverantörens tjänster.

25. Vid uppdragsavtal för ej kritiska eller ej viktiga operativa funktioner eller verksamheter bör företaget definiera den information som ska registreras baserat på art, omfattning och komplexitet för riskerna med de tjänster som molntjänstleverantören tillhandahåller.

26. På förfrågan bör företaget göra all information tillgänglig för tillsynsmyndigheten för att göra det möjligt för den att övervaka företaget, inbegripet en kopia av uppdragsavtalet.

Riktlinje 6 – Analys innan uppdragsavtal ingås

27. Innan några överenskommelser ingås med molntjänstleverantörer bör företaget

a. bedöma om överenskommelsen om uppdragsavtal om molntjänster avser en kritisk eller viktig operativ funktion eller verksamhet i enlighet med riktlinje 7,

b. identifiera och bedöma alla relevanta risker med överenskommelsen om uppdragsavtal om molntjänster i enlighet med riktlinje 8,

c. genomföra en lämplig företagsbesiktning av den blivande molntjänstleverantören i enlighet med riktlinje 9,

d. identifiera och bedöma intressekonflikter som uppdragsavtalet kan orsaka i enlighet med kraven i artikel 274.3 b i den delegerade förordningen.

Riktlinje 7 – Bedömning av kritiska eller viktiga operativa funktioner och verksamheter

28. Innan några överenskommelser om uppdragsavtal ingås med molntjänstleverantörer bör företaget bedöma om överenskommelsen om uppdragsavtal om molntjänster avser en operativ funktion eller verksamhet som är kritisk eller viktig. När bedömningen görs bör företaget, om så är relevant, överväga huruvida överenskommelsen har potential att bli kritisk eller viktig i framtiden. Företaget bör också ompröva huruvida en operativ funktion eller verksamhet som tidigare har lagts ut på molntjänstleverantörer fortsätter att vara kritisk eller viktig om avtalets risker förändras avsevärt i fråga om riskernas art, omfattning eller komplexitet.

29. I bedömningen bör företaget beakta åtminstone följande faktorer, tillsammans med riskbedömningens resultat:

a. Hur varje eventuell väsentlig störning i den operativa funktion eller verksamhet som omfattas av uppdragsavtal, eller misslyckande från molntjänstleverantören med att tillhandahålla tjänsterna kontinuerligt på de överenskomna servicenivåerna, påverkar företagets

   i. kontinuerliga efterlevnad av de lagstadgade kraven,

   ii. kort- och långsiktiga motståndskraft och bärkraft vad gäller ekonomi och solvens,

   iii. affärskontinuitet och operativa motståndskraft,

   iv. operativa risk, inbegripet vad gäller uppförande, IKT och juridiska risker,

   v. ryktesrisker.

b. Hur överenskommelsen om uppdragsavtal om molntjänster potentiellt påverkar företagets möjlighet att

   i. identifiera, övervaka och hantera alla relevanta risker,

   ii. efterleva alla juridiska krav och regleringskrav,

   iii. genomföra lämpliga revisioner av den operativa funktion eller verksamhet som omfattas av uppdragsavtal.

c. Företagets (och/eller gruppens i tillämpliga fall) sammanlagda exponering för samma molntjänstleverantör och den potentiella kumulativa påverkan från överenskommelser om uppdragsavtal om molntjänster i samma affärsområde.

d. Storleken och komplexiteten på företagets affärsområden som påverkas av överenskommelsen om uppdragsavtal om molntjänster.

e. Möjligheten att vid behov eller om så önskas överföra den föreslagna överenskommelsen om uppdragsavtal om molntjänster till en annan molntjänstleverantör eller återintegrera tjänsterna (”utbytbarhet”).

f. Skyddet av personuppgifter och icke-personuppgifter samt hur företaget, försäkringstagare eller andra relevanta intressenter potentiellt påverkas av brott mot konfidentialiteten eller misslyckande att säkerställa uppgifternas tillgänglighet och integritet med utgångspunkt i bland annat förordning (EU) 2016/679[7]. Företaget bör i synnerhet beakta uppgifter som utgör affärshemligheter och/eller är känsliga (till exempel uppgifter om försäkringstagares hälsa).

Riktlinje 8 – Riskbedömning av uppdragsavtal om molntjänster

30. I allmänhet bör företaget tillämpa en strategi som är proportionerlig till art, omfattning och komplexitet för riskerna med tjänsterna som läggs ut på molntjänstleverantörer. Detta inbegriper att bedöma hur uppdragsavtal om molntjänster i synnerhet kan påverka operativa risker och ryktesrisker.

31. Vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer bör ett företag

a. beakta de förväntade fördelarna och kostnaderna för den föreslagna överenskommelsen om uppdragsavtal om molntjänster, och samtidigt väga avsevärda risker som kan minskas eller hanteras bättre mot avsevärda risker som kan uppstå till följd av den föreslagna överenskommelsen om uppdragsavtal om molntjänster,

b. om så är tillämpligt och lämpligt bedöma riskerna, inbegripet rättsliga risker samt IKT-, efterlevnads- och ryktesrisker samt tillsynsbegränsningar som uppstår från

   i. den valda molntjänsten och den föreslagna distributionsmodellen (dvs. offentligt moln/privat moln/hybridmoln/gemenskapsmoln),

   ii. migreringen och/eller genomförandet,

   iii. verksamheten och de tillhörande uppgifter som eventuellt ska omfattas av uppdragsavtal (eller redan gör det) och deras känslighet och nödvändiga säkerhetsåtgärder,

   iv. den politiska stabiliteten och säkerhetssituationen i de länder (i eller utanför EU) där de tjänster som omfattas av uppdragsavtal tillhandahålls eller kan tillhandahållas och där uppgifterna lagras eller sannolikt kommer att lagras. Bedömningen bör beakta

      1. gällande lagar, inklusive lagar för dataskydd,

      2. vilka bestämmelser för brottsbekämpning som finns,

      3. den insolvenslagstiftning som skulle gälla i händelse av en tjänsteleverantörs fallering och eventuella hinder som skulle uppkomma i samband med brådskande återhämtning av företagets uppgifter,

[7] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), EUT L 119, 4.5.2016, s. 1.

v. underentreprenad, inbegripet de ytterligare risker som kan uppstå om underleverantören finns i ett tredjeland eller ett annat land än molntjänstleverantören och risken för att långa och komplexa underentreprenörskedjor minskar företagets förmåga att övervaka sina kritiska eller viktiga operativa funktioner eller verksamheter och tillsynsmyndigheternas förmåga att effektivt övervaka dem,

vi. företagets övergripande koncentrationsrisk till samma molntjänstleverantör, inbegripet uppdragsavtal med en molntjänstleverantör som inte enkelt kan ersättas eller flera överenskommelser om uppdragsavtal med samma molntjänstleverantör. Vid bedömning av koncentrationsrisken bör företaget (och/eller gruppen, i tillämpliga fall) beakta alla överenskommelser om uppdragsavtal om molntjänster med den molntjänstleverantören.

32. Riskbedömningen bör genomföras innan en överenskommelse om uppdragsavtal om molntjänster ingås. Om företaget blir medvetet om betydande brister och/eller betydande förändringar i de tjänster som tillhandahålls eller i molntjänstleverantörens situation bör riskbedömningen ses över eller göras om snarast. Om en överenskommelse om uppdragsavtal om molntjänster förnyas avseende innehåll och omfattning (till exempel utökning av omfattningen eller inkluderande av kritiska eller viktiga operativa funktioner som tidigare inte inkluderats i omfattningen) bör riskbedömningen göras om.

Riktlinje 9 – Företagsbesiktning av molntjänstleverantören

33. Företaget bör i sin urvals- och bedömningsprocess säkerställa att molntjänstleverantören är lämplig enligt de kriterier som fastställs i dess skriftliga policy om uppdragsavtal.

34. Företagsbesiktningen av molntjänstleverantören bör genomföras innan uppdragsavtal ingås för en operativ funktion eller verksamhet. Om företaget ingår ett andra avtal med en molntjänstleverantör som redan har bedömts bör företaget utifrån en riskbaserad strategi fastställa om en andra företagsbesiktning krävs. Om företaget blir medvetet om betydande brister och/eller betydande förändringar i de tjänster som tillhandahålls eller i molntjänstleverantörens situation bör företagsbesiktningen ses över eller göras om snarast.

35. Vid uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner bör företagsbesiktningen innefatta en utvärdering av molntjänstleverantörens lämplighet (till exempel kompetenser, infrastruktur, ekonomisk situation, företags- och tillsynsstatus). Om så är lämpligt kan företaget använda bevisning, certifieringar baserade på internationella standarder, revisionsrapporter från erkända tredje parter eller interna revisionsrapporter till stöd för företagsbesiktningen.

Riktlinje 10 – Avtalsenliga krav

36. Företagets och molntjänstleverantörens rättigheter och skyldigheter bör vara klart och tydligt fördelade och specificerade i ett skriftligt avtal.

37. Utan att det påverkar kraven i artikel 274 i den delegerade förordningen bör följande fastställas i det skriftliga avtalet mellan företaget och molntjänstleverantören vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter med en molntjänstleverantör:

a. En tydlig beskrivning av den tillhandahållna funktion som omfattas av uppdragsavtal (molntjänster, inbegripet typen av stödtjänster).

b. Startdatum och slutdatum, i tillämpliga fall, för avtalet och uppsägningstiden för molntjänstleverantören och företaget.

c. Domstol för tvistemål och tillämplig lagstiftning för avtalet.

d. Parternas finansiella skyldigheter.

e. Huruvida underentreprenad för en kritisk eller viktig operativ funktion eller verksamhet (eller avsevärda delar därav) tillåts och om så är fallet vilka villkor som gäller för väsentlig underentreprenad (se riktlinje 13).

f. Den eller de platser (dvs. regioner eller länder) där relevanta uppgifter kommer att lagras och behandlas (datacentrens lokalisering) och de villkor som ska uppfyllas, inbegripet ett krav om att meddela företaget om tjänsteleverantören föreslår att ändra platsen eller platserna.

g. Bestämmelser om relevanta uppgifters tillgänglighet, integritet, konfidentialitet, sekretess och säkerhet, med beaktande av specifikationerna i riktlinje 12.

h. Företagets rätt att regelbundet övervaka molntjänstleverantörens prestationer.

i. De överenskomna servicenivåerna, som bör inkludera exakta kvantitativa och kvalitativa resultatmål för att möjliggöra övervakning i god tid så att lämpliga korrigerande åtgärder kan vidtas utan onödigt dröjsmål om de överenskomna servicenivåerna inte uppfylls.

j. Molntjänstleverantörens rapporteringsskyldigheter gentemot företaget, inbegripet, om så är lämpligt, skyldigheterna att lämna in rapporter som är relevanta för företagets säkerhetsfunktion och viktiga funktioner, såsom rapporter från molntjänstleverantörens internrevisionsfunktion.

k. Huruvida molntjänstleverantören bör teckna en obligatorisk försäkring mot vissa risker och, i tillämpliga fall, vilken nivå på försäkringsskydd som efterfrågas.

l. Kraven på att införa och testa affärskontinuitetsplaner.

m. Kravet på att molntjänstleverantören ska ge företaget, dess tillsynsmyndigheter och andra personer som utses av företaget eller tillsynsmyndigheterna följande:

    i. Fullständigt tillträde till alla relevanta företagslokaler (huvudkontor och operativa centraler), inklusive hela utbudet av relevanta enheter, system, nätverk, information och uppgifter som används för att tillhandahålla den funktion som omfattas av uppdragsavtal, däribland anknuten finansiell information, personal och molntjänstleverantörens utomstående revisorer (”åtkomsträttigheter”).

    ii. Obegränsad rätt till inspektion och revision gällande överenskommelsen om uppdragsavtal om molntjänster (”revisionsrättigheter”) så att de kan övervaka överenskommelsen om uppdragsavtal och säkerställa att alla tillämpliga lagstadgade och avtalsenliga krav efterlevs.

n. Bestämmelser som säkerställer att de uppgifter som ägs av företaget är möjliga för företaget att få tillgång till i händelse av insolvens, resolution eller upphörd affärsverksamhet för molntjänstleverantören.

Riktlinje 11 – Åtkomst- och revisionsrättigheter

38. Uppdragsavtalet om molntjänster bör inte begränsa företagets effektiva utövande av åtkomst- och revisionsrättigheter samt kontrollalternativ för molntjänster i syfte att fullgöra de lagstadgade skyldigheterna.

39. Företaget bör utöva sina åtkomst- och revisionsrättigheter, fastställa hur ofta revisioner ska genomföras och de områden och tjänster som ska granskas utifrån en riskbaserad strategi, i enlighet med avsnitt 8 i Eiopas riktlinjer för företagsstyrningssystem.

40. När företaget fastställer hur ofta och i vilken omfattning det ska utöva sina åtkomst- eller revisionsrättigheter bör företaget beakta huruvida uppdragsavtalet om molntjänster avser en kritisk eller viktig operativ funktion eller verksamhet, riskernas art och omfattning samt påverkan på företaget genom överenskommelserna om uppdragsavtal om molntjänster.

41. Om utövandet av åtkomst- och revisionsrättigheterna eller användningen av vissa revisionstekniker skapar en risk för molntjänstleverantörens miljö och/eller en annan molntjänstleverantörs kund (till exempel påverkan på servicenivåer, uppgifters tillgänglighet, konfidentialitetsaspekter) bör företaget och molntjänstleverantören komma överens om alternativa sätt att tillhandahålla en liknande tillförlitlighets- och servicenivå till företaget (till exempel inbegripande av specifika kontroller som ska testas i en specifik rapport/certifiering som molntjänstleverantören skapar).

42. Utan att det påverkar företagets slutliga ansvar för de verksamheter som utförs av molntjänstleverantörerna kan företaget, i syfte att tillämpa revisionsresurser effektivare och minska den organisatoriska bördan för molntjänstleverantören och dess kunder, använda

a. tredjepartscertifieringar och tredjepartsrevisionsrapporter eller interna revisionsrapporter som har gjorts tillgängliga av molntjänstleverantören,

b. gemensamma revisioner (dvs. revisioner som utförs tillsammans med andra av molntjänstleverantörens kunder) eller gemensamma revisioner som utförs av en tredje part som företaget utser.

43. Vid uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter bör företag tillämpa den metod som beskrivs i punkt 42 a endast om de

a. ser till att certifieringen eller revisionsrapporten omfattar de system (till exempel processer, applikationer, infrastruktur, datacenter osv.) och de kontroller som identifierats av företaget samt bedömer efterlevnad av relevanta regleringskrav,

b. noggrant och regelbundet bedömer innehållet i nya certifieringar eller revisionsrapporter och kontrollerar att certifieringarna eller rapporterna inte är inaktuella,

c. säkerställer att centrala system och kontroller omfattas i framtida versioner av certifieringen eller revisionsrapporten,

d. är tillfreds med den certifierande eller reviderande partens lämplighet (till exempel med avseende på rotation av det certifierande eller reviderande företaget, kvalifikationerna, expertisen, de upprepade kontrollerna/verifieringen av bevisen i den underliggande revisionsakten),

e. är tillfreds med att certifieringar utfärdas och att revisionerna utförs på grundval av lämpliga standarder och inbegriper ett test av den operativa effektiviteten hos de centrala kontroller som har införts,

f. har den avtalsenliga rätten att begära att omfattningen av certifieringarna eller revisionsrapporterna utökas till andra relevanta system och kontroller; antalet sådana begäranden om ändrad omfattning och hur ofta de görs bör vara rimligt och motiverat ur ett riskhanteringsperspektiv,

g. behåller den avtalsenliga rätten att genomföra enskilda revisioner på plats efter eget gottfinnande avseende uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter. Denna rätt bör utövas vid specifika behov som inte kan tillfredsställas genom andra typer av interaktion med molntjänstleverantören.

44. Vid uppdragsavtal med molntjänstleverantörer för kritiska eller viktiga operativa funktioner bör företaget bedöma om de tredjepartscertifieringar och tredjepartsrapporter som avses i punkt 42 a är adekvata och tillräckliga för att uppfylla deras lagstadgade skyldigheter, och bör utifrån en riskbaserad strategi inte förlita sig enbart på dessa rapporter och certifieringar med tiden.

45. Före ett planerat besök på plats bör den part som utövar sin åtkomsträttighet (företag, revisor eller tredje part som agerar på företagets eller företagens vägnar) meddela detta inom en rimlig tidsperiod, om inte ett tidigt förhandsmeddelande är omöjligt på grund av en nöd- eller krissituation. Ett sådant meddelande bör innefatta platsen för besöket och dess syfte samt den personal som kommer att närvara vid besöket.

46. Mot bakgrund av att molnlösningar har en hög teknisk komplexitet bör företaget kontrollera att den personal som utför revisionen – företagets interna revisorer eller den grupp revisorer som agerar på dess vägnar, eller molntjänstleverantörens utsedda revisorer – eller, i förekommande fall, den personal som granskar tredjepartscertifieringar eller tjänsteleverantörens revisionsrapporter har lämplig kompetens och kunskap för att utföra relevanta revisioner och/eller bedömningar.

Riktlinje 12 – Uppgifts- och systemsäkerhet

47. Företaget bör säkerställa att molntjänstleverantörerna efterlever europeiska och nationella föreskrifter samt lämpliga IKT-säkerhetsstandarder.

48. Vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer bör företaget dessutom definiera särskilda informationssäkerhetskrav i uppdragsavtalet och regelbundet övervaka efterlevnaden av dessa krav.

49. Vad beträffar punkt 48 bör företaget, vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer, utifrån en riskbaserad strategi och med beaktande av sitt ansvar samt molntjänstleverantörens ansvar

a. komma överens om tydliga roller och ansvarsområden för molntjänstleverantören och företaget avseende de operativa funktioner eller verksamheter som påverkas av uppdragsavtalet om molntjänster och fördelningen bör vara tydlig,

b. definiera och besluta om en lämplig skyddsnivå för konfidentiella uppgifter, kontinuiteten för de verksamheter som ska omfattas av uppdragsavtal samt integriteten och spårbarheten för data och system mot bakgrund av det avsedda uppdragsavtalet om molntjänster,

c. överväga särskilda åtgärder om så behövs för transiterande, minnesbelägna och vilande data, till exempel användning av krypteringstekniker i kombination med en lämplig nyckelhantering,

d. överväga molntjänsternas integreringsmekanismer med företagens system, till exempel gränssnitten för tillämpningsprogram och en sund användar- och åtkomsthanteringsprocess,

e. i avtalet säkerställa att nätverkstrafikens tillgänglighet och förväntade kapacitet efterlever höga kontinuitetskrav, om så är tillämpligt och rimligt,

f. definiera och besluta om lämpliga kontinuitetskrav som säkerställer lämpliga nivåer på varje nivå i den tekniska kedjan, i tillämpliga fall,

g. ha en sund och väldokumenterad hanteringsprocess för tillbud, inbegripet respektive ansvarsområden, till exempel genom att definiera en samarbetsmodell om faktiska eller misstänkta tillbud inträffar,

h. anta en riskbaserad strategi för platser för lagring och hantering av uppgifter (dvs. land eller region) och informationssäkerhetsbeaktanden,

i. övervaka efterlevnaden av kraven på ändamålsenligheten och effektiviteten hos de kontrollmekanismer som molntjänstleverantören genomför och som skulle minska riskerna för de tillhandahållna tjänsterna.

Riktlinje 13 – Underentreprenad för kritiska eller viktiga operativa funktioner eller verksamheter

50. Om underentreprenad tillåts för kritiska eller viktiga operativa funktioner (eller en del därav) bör uppdragsavtalet om molntjänster mellan företaget och molntjänstleverantören

a. ange alla typer av verksamhet som är undantagna från eventuell underentreprenad,

b. specificera de villkor som ska efterlevas vid underentreprenad (till exempel att underleverantören också fullt ut ska efterleva molntjänstleverantörens relevanta skyldigheter); dessa skyldigheter inbegriper revisions- och åtkomsträttigheter samt uppgifts- och systemsäkerhet,

c. specificera att molntjänstleverantören behåller fullt ansvar och full tillsyn för de tjänster som läggs ut på underentreprenad,

d. innehålla en skyldighet för molntjänstleverantören att informera företaget om alla planerade betydande förändringar när det gäller de underleverantörer eller de tjänster som lagts ut på underentreprenad och som kan påverka tjänsteleverantörens möjlighet att uppfylla sina skyldigheter i enlighet med uppdragsavtalet om molntjänster. Delgivningsperioden för dessa förändringar bör göra det möjligt för företaget att åtminstone utföra en riskbedömning av de föreslagna ändringarnas inverkan innan den faktiska förändringen rörande underleverantörer eller de tjänster som lagts ut på underentreprenad träder i kraft,

e. säkerställa att företaget har rätt att invända mot förändringarna och/eller säga upp avtalet, om en molntjänstleverantör planerar förändringar när det gäller de underleverantörer eller de tjänster som lagts ut på underentreprenad som skulle ha en negativ effekt på riskbedömningen av de avtalade tjänsterna.

Riktlinje 14 – Övervakning och översyn av överenskommelser om uppdragsavtal om molntjänster

51. Företaget bör regelbundet övervaka molntjänstleverantörens utförande av verksamheter, säkerhetsåtgärder och efterlevnad av överenskommen servicenivå utifrån en riskbaserad strategi. Det huvudsakliga fokuset bör ligga på uppdragsavtal om molntjänster för kritiska och viktiga operativa funktioner.

52. För att uppnå detta bör företaget inrätta övervaknings- och översynsmekanismer som, om så är rimligt och lämpligt, bör beakta om kritiska eller viktiga operativa funktioner eller en del därav läggs ut på underentreprenad.

53. Förvaltnings-, ledningss- eller tillsynsorganet bör regelbundet uppdateras om de risker som identifieras i uppdragsavtalet om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter.

54. I syfte att säkerställa lämplig övervakning och översyn av överenskommelserna om uppdragsavtal om molntjänster bör företagen tillämpa tillräckliga resurser med lämplig kompetens och kunskap för övervakning av de tjänster som omfattas av uppdragsavtal för molnet. Företagets personal som ansvarar för dessa verksamheter bör ha både IKT- och branschkunskap i nödvändig utsträckning.

Riktlinje 15 – Rätt till uppsägning och utträdesstrategier

55. Vid uppdragsavtal för molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter bör företaget inom ramen för uppdragsavtalet för molntjänster ha en tydligt definierad utträdesstrategiklausul som säkerställer att det vid behov kan säga upp överenskommelsen. Uppsägningen ska möjliggöras utan förfång för kontinuiteten och kvaliteten på leveransen av tjänster till försäkringstagarna. För att uppnå detta bör företaget

a. ta fram utträdesplaner som är omfattande, tjänstebaserade, dokumenterade och tillräckligt testade (till exempel genom att genomföra en analys av de potentiella kostnaderna, effekterna, resurserna och tidskonsekvenserna för de olika potentiella utträdesalternativen),

b. identifiera alternativa lösningar och ta fram lämpliga och rimliga övergångsplaner som gör det möjligt för företaget att ta bort och överföra befintliga verksamheter och uppgifter från molntjänstleverantören till alternativa tjänsteleverantörer eller tillbaka till företaget. Dessa lösningar bör definieras mot bakgrund av de utmaningar som kan uppstå på grund av uppgifternas lokalisering och nödvändiga åtgärder bör vidtas för att säkerställa affärskontinuitet under övergångsfasen,

c. säkerställa att molntjänstleverantören på ett lämpligt sätt stöder företaget vid överföringen av uppgifterna, systemen eller applikationerna som omfattas av uppdragsavtal till en annan tjänsteleverantör eller direkt till företaget,

d. komma överens med molntjänstleverantören om att molntjänstleverantören ska radera företagets uppgifter fullständigt och säkert i alla regioner när dessa har återförts till företaget.

56. När företaget utarbetar utträdesstrategier bör det tänka på följande:

a. Definiera målsättningarna i utträdesstrategin.

b. Definiera de triggerhändelser (till exempel viktiga riskindikatorer som rapporterar om en oacceptabel tjänstenivå) som kan aktivera utträdesstrategin.

c. Utföra en verksamhetsanalys som står i proportion till de verksamheter som omfattas av uppdragsavtal för att utröna vilka mänskliga och övriga resurser som krävs för att genomföra utträdesplanen och hur lång tid detta skulle ta.

d. Tilldela roller och ansvarsområden för hantering av utträdesplaner och övergångsverksamheter.

e. Definiera kriterier för att fastställa om övergången har lyckats.

Riktlinje 16 – Tillsyn av överenskommelser om uppdragsavtal om molntjänster av tillsynsmyndigheter

57. Tillsynsmyndigheterna bör analysera inverkan från företagens överenskommelser om uppdragsavtal om molntjänster som en del av tillsynens granskningsprocess. Fokus i analysen av inverkan bör i synnerhet ligga på överenskommelser som avser uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter.

58. Tillsynsmyndigheterna bör överväga följande risker i tillsynen av företagens överenskommelser om uppdragsavtal om molntjänster:

a. IKT-risker.

b. Andra operativa risker (inbegripet rättsliga risker och efterlevnadsrisker, risker avseende hantering av uppdragsavtal och tredje part).

c. Ryktesrisker.

d. Koncentrationsrisker, inbegripet på lands-/sektorsnivå.

59. Inom ramen för sin bedömning bör tillsynsmyndigheterna inkludera följande aspekter utifrån en riskbaserad strategi:

a. Lämpligheten och effektiviteten i företagets styrningsprocesser och operativa processer när det gäller godkännande, genomförande, övervakning, hantering och förnyelse av överenskommelser om uppdragsavtal om molntjänster.

b. Huruvida företaget har tillräckliga resurser med lämplig kompetens och kunskap för att övervaka de tjänster som omfattas av uppdragsavtal för molnet.

c. Huruvida företaget identifierar och hanterar alla risker som belyses i dessa riktlinjer.

60. Avseende grupper bör grupptillsynsmyndigheten säkerställa att inverkan från uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter återspeglas i gruppens tillsynsriskbedömning, med beaktande av kraven som listas i punkterna 58–59 och gruppens enskilda styrningsegenskaper och operativa egenskaper.

61. Om uppdragsavtal om molntjänster för kritiska eller viktiga operativa funktioner eller verksamheter inbegriper mer än ett företag i olika medlemsstater och förvaltas centralt av moderföretaget eller av ett dotterbolag (till exempel ett företag eller ett grupptjänsteföretag såsom gruppens IKT-leverantör) bör grupptillsynsmyndigheten och/eller relevanta tillsynsmyndigheter för de företag som inbegrips av uppdragsavtalet om molntjänster i tillämpliga fall diskutera inverkan från uppdragsavtalet om molntjänster på gruppens riskprofil i tillsynskollegiet.

62. När det konstateras orosmoment som leder till slutsatsen att ett företag inte längre har stabila styrformer inrättade eller inte efterlever regleringskrav, bör tillsynsmyndigheterna vidta lämpliga åtgärder, vilka till exempel kan innefatta att begära att företaget förbättrar styrningsarrangemanget, att begränsa omfattning för

de funktioner som omfattas av uppdragsavtal eller att kräva utträde ur en eller flera överenskommelser om uppdragsavtal. I synnerhet, med hänsyn till företagets behov av kontinuitet i verksamheten, skulle upphävda kontrakt kunna krävas om tillsynen och verkställigheten av regleringskrav inte kan säkerställas genom andra åtgärder.

Regler för efterlevnad och rapportering

63. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1094/2010. I enlighet med artikel 16.3 i denna förordning ska behöriga myndigheter och finansinstitut med alla tillgängliga medel söka följa dessa riktlinjer och rekommendationer.

64. De behöriga myndigheter som följer eller har för avsikt att följa dessa riktlinjer bör införliva dem i sina ramar för regler och tillsyn på ett lämpligt sätt.

65. De behöriga myndigheterna ska, inom två månader från det att de översatta versionerna har offentliggjorts, bekräfta till Eiopa om huruvida de följer eller avser att följa dessa riktlinjer, och ange skälen till att de eventuellt inte följer dem.

66. Om Eiopa inte har fått något svar inom denna tidsfrist kommer behöriga myndigheter att anses inte följa rapporteringen och rapporteras i enlighet med detta.

Slutbestämmelse om översyn

67. Dessa riktlinjer ska vara föremål för översyn av Eiopa.