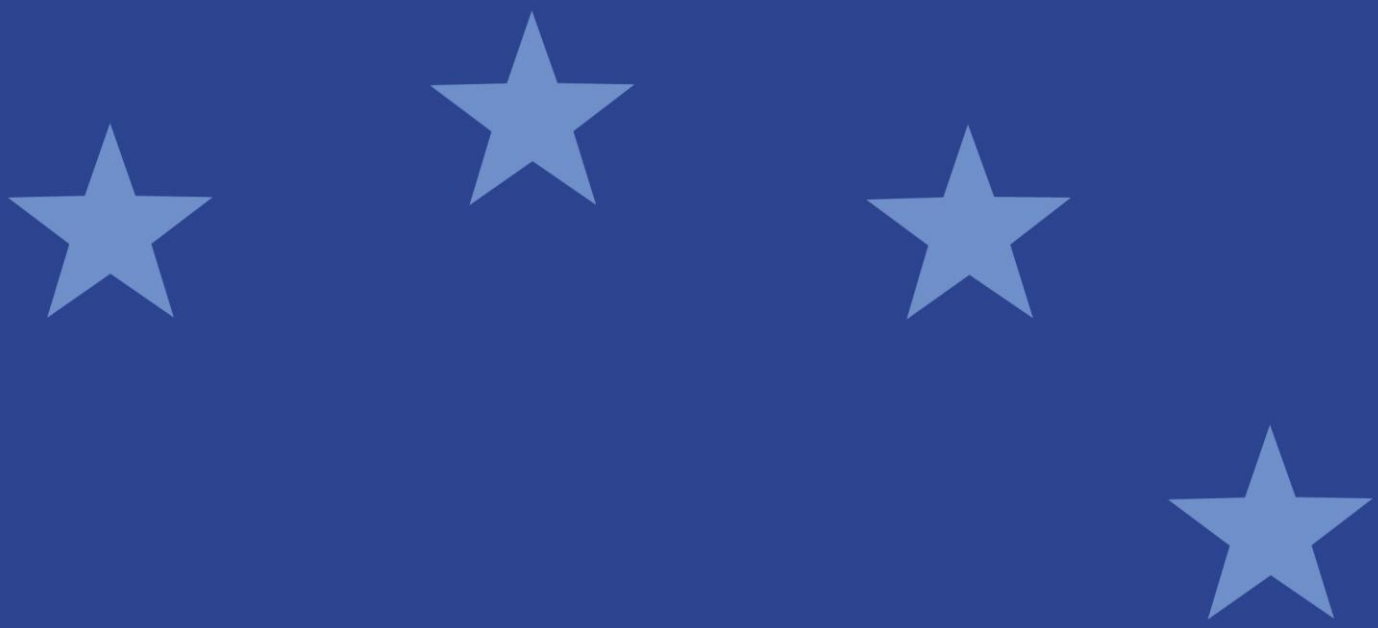
esma European Securities and Markets Authority

Riktlinjer

för utkontraktering till molntjänstleverantörer



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

Innehållsförteckning

I. Tillämpningsområde

Mottagare

1. Dessa riktlinjer är relevanta för behöriga myndigheter och avsedda för finansinstitut, vilket i den mening som avses i dessa riktlinjer omfattar i) förvaltare av alternativa investeringsfonder (AIF-förvaltare) och förvaringsinstitut för alternativa investeringsfonder (AIF-fonder), ii) företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag), fondföretags förvaltningsbolag och förvaringsinstitut samt investeringsbolag som inte har utsett ett förvaltningsbolag som auktoriserats i enlighet med fondföretagsdirektivet, iii) centrala motparter inklusive centrala motparter från tredjeland som uppfyller tillämpliga krav i Emir, iv) transaktionsregister, v) värdepappersföretag och kreditinstitut för investeringstjänster och investeringsverksamhet, leverantörer av datarapporteringstjänster och handelsplatsers marknadsoperatörer, vi) värdepapperscentraler, vii) kreditvärderingsinstitut, viii) värdepapperiseringsregister och ix) administratörer av kritiska referensvärden.

2. Esma kommer också att beakta dessa riktlinjer när den bedömer i vilken utsträckning en central motpart från tredjeland uppfyller de tillämpliga kraven i Emir genom att uppfylla jämförbara krav i tredjelandet i enlighet med artikel 25.2b a i Emir.

Tillämpningsområde

3. Dessa riktlinjer avser följande bestämmelser:

   a) Artiklarna 15, 18, 20 och 21.8 i direktivet om AIF-förvaltare; artiklarna 13, 22, 38, 39, 40, 44, 45, 57.1 d, 57.2, 57.3, 58, 75, 76, 77, 79, 81, 82 och 98 i kommissionens delegerade förordning (EU) nr 231/2013.
   b) Artiklarna 12.1 a, 13, 14.1 c, 22, 22a, 23.2, 30 och 31 i fondföretagsdirektivet; artiklarna 4.1 till 4.3, 4.5, 5.2, 7, 9, 23.4, 32, 38, 39 och 40 i kommissionens direktiv 2010/43/EU; artiklarna 2.2 j, 3.1, 13.2, 15, 16 och 22 i kommissionens delegerade förordning (EU) 2016/438.
   c) Artiklarna 25, 26.1, 26.3, 26.6, 34, 35 och 78–81 i Emir; artiklarna 5 och 12 i förordningen om transparens i transaktioner för värdepappersfinansiering; artiklarna 3.1 f, 3.2, 4, 7.2 d och f, 9 och 17 i kommissionens delegerade förordning (EU) nr 153/2013; artiklarna 16 och 21 i kommissionens delegerade förordning (EU) nr 150/2013; artiklarna 16 och 21 i kommissionens delegerade förordning (EU) 2019/359.

d) Artiklarna 16.2, 16.4, 16.5, 18.1, 19.3 a, 47.1 b och c, 48.1, 64.4, 65.5 och 66.31 i Mifid II; artiklarna 21.1 till 21.3, 23, 29.5, 30, 31 och 32 i kommissionens delegerade förordning (EU) 2017/565; artiklarna 6, 15 och 16.6 i kommissionens delegerade förordning (EU) 2017/584; artiklarna 6, 7, 8 och 9 i kommissionens delegerade förordning (EU) 2017/571.
e) Artiklarna 22, 26, 30, 42, 44 och 45 i CSD-förordningen samt artiklarna 33, 47, 50.1, 57.2 i, 66, 68, 75, 76, 78 och 80 i kommissionens delegerade förordning (EU) 2017/392.
f) Artikel 9 och bilaga I avsnitt A punkterna 4 och 8 samt punkt 17 i bilaga II till förordningen om kreditvärderingsinstitut och artiklarna 11 och 25 i kommissionens delegerade förordning (EU) nr 449/2012.
g) Artikel 10.2 i förordningen om värdepapperisering.
h) Artiklarna 6.3 och 10 i referensvärdesförordningen och punkt 7 i bilaga I till kommissionens delegerade förordning (EU) 2018/1646.

Tillämpningsdatum

4. Dessa riktlinjer gäller från och med den 31 juli 2021 för alla uppdragsavtal om molntjänster som ingås, förnyas eller ändras på eller efter detta datum. Företagen bör se över och ändra befintliga uppdragsavtal om molntjänster för att se till att de tar hänsyn till dessa riktlinjer senast den 31 december 2022. Om granskningen av uppdragsavtal om molntjänster för kritiska eller viktiga funktioner inte är färdig till den 31 december 2022 ska företagen informera behöriga myndigheter om detta, samt om vilka åtgärder som planeras för att fullgöra granskningen eller den eventuella utträdesstrategin.

II. Hänvisningar till lagstiftning, förkortningar och definitioner

Hänvisningar till lagstiftning

Esmaförordningen	Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG[2]
Direktivet om AIF-förvaltare	Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv

[1] Från och med den 1 januari 2022 bör hänvisningen till artiklarna 64.4, 65.5 och 66.3 i Mifid II tolkas som en hänvisning till artiklarna 27g.4, 27h.5 och 27i.3 i Mifir.
[2] EUT L 331, 15.12.2010, s. 84.

	2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010[3]
Kommissionens delegerade förordning (EU) nr 231/2013	Kommissionens delegerade förordning (EU) nr 231/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets direktiv 2011/61/EU vad gäller undantag, allmänna verksamhetsvillkor, förvaringsinstitut, finansiell hävstång, öppenhet och tillsyn[4]
Fondföretagsdirektivet	Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag)[5]
Kommissionens direktiv 2010/43/EU	Kommissionens direktiv 2010/43/EU av den 1 juli 2010 om genomförande av Europaparlamentets och rådets direktiv 2009/65/EG när det gäller organisatoriska krav, intressekonflikter, uppföranderegler, riskhantering och innehållet i avtalet mellan ett förvaringsinstitut och ett förvaltningsbolag[6]
Kommissionens delegerade förordning (EU) 2016/438	Kommissionens delegerade förordning (EU) 2016/438 av den 17 december 2015 om komplettering av Europaparlamentets och rådets direktiv 2009/65/EG vad gäller krav avseende förvaringsinstitut[7]
Emir	Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister[8]
Förordningen om transparens i transaktioner för värdepappersfinansiering	Europaparlamentets och rådets förordning (EU) 2015/2365 av den 25 november 2015 om transparens i transaktioner för värdepappersfinansiering och om återanvändning samt om ändring av förordning (EU) nr 648/2012[9]
Kommissionens delegerade förordning (EU) nr 153/2013	Kommissionens delegerade förordning (EU) nr 153/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 med avseende på tekniska tillsynsstandarder för krav på centrala motparter[10]

[3] EUT L 174, 1.7.2011, s. 1.
[4] EUT L 83, 22.3.2013, s. 1.
[5] EUT L 302, 17.11.2009, s. 32.
[6] EUT L 176, 10.7.2010, s. 42.
[7] EUT L 78, 24.3.2016, s. 11.
[8] EUT L 201, 27.7.2012, s. 1.
[9] EUT L 337, 23.12.2015, s. 1.
[10] EUT L 52, 23.2.2013, s. 41.

Kommissionens delegerade förordning (EU) nr 150/2013	Kommissionens delegerade förordning (EU) nr 150/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 om OTC-derivat, centrala motparter och transaktionsregister med avseende på tekniska standarder för tillsyn som anger vilka uppgifter som ska finnas i en ansökan om registrering som transaktionsregister[11]
Kommissionens delegerade förordning (EU) 2019/359	Kommissionens delegerade förordning (EU) 2019/359 av den 13 december 2018 om komplettering av Europaparlamentets och rådets förordning (EU) 2015/2365 vad gäller tekniska tillsynsstandarder som specificerar de uppgifter som ska lämnas i ansökningar om registrering och utvidgning av registrering som transaktionsregister[12]
Mifid II	Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU[13]
Mifir	Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012[14]
Kommissionens delegerade förordning (EU) 2017/565	Kommissionens delegerade förordning (EU) 2017/565 av den 25 april 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU vad gäller organisatoriska krav och villkor för verksamheten i värdepappersföretag, och definitioner för tillämpning av det direktivet[15]
Kommissionens delegerade förordning (EU) 2017/584	Kommissionens delegerade förordning (EU) 2017/584 av den 14 juli 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder som specificerar organisatoriska krav för handelsplatser[16]
Kommissionens delegerade förordning (EU) 2017/571	Kommissionens delegerade förordning (EU) 2017/571 av den 2 juni 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder när det gäller

[11] EUT L 52, 23.2.2013, s. 25.
[12] EUT L 81, 22.3.2019, s. 45.
[13] EUT L 173, 12.6.2014, s. 349.
[14] EUT L 173, 12.6.2014, s. 84.
[15] EUT L 87, 31.3.2017, s. 1.
[16] EUT L 87, 31.3.2017, s. 350.

	auktorisation, organisatoriska krav och publicering av transaktioner för leverantörer av datarapporteringstjänster[17]
CSD-förordningen	Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012[18]
Kommissionens delegerade förordning (EU) 2017/392	Kommissionens delegerade förordning (EU) 2017/392 av den 11 november 2016 om komplettering av Europaparlamentets och rådets förordning (EU) nr 909/2014 med avseende på tekniska tillsynsstandarder för auktorisationskrav, tillsynskrav och operativa krav för värdepapperscentraler[19]
Förordningen om kreditvärderingsinstitut	Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut[20]
Kommissionens delegerade förordning (EU) nr 449/2012	Kommissionens delegerade förordning (EU) nr 449/2012 av den 21 mars 2012 om komplettering av Europaparlamentets och rådets förordning (EG) nr 1060/2009 med avseende på tekniska tillsynsstandarder för uppgiftslämning vid registrering och certifiering av kreditvärderingsinstitut[21]
Förordningen om värdepapperisering	Europaparlamentets och rådets förordning (EU) 2017/2402 av den 12 december 2017 om ett allmänt ramverk för värdepapperisering och om inrättande av ett särskilt ramverk för enkel, transparent och standardiserad värdepapperisering samt om ändring av direktiven 2009/65/EG, 2009/138/EG och 2011/61/EU och förordningarna (EG) nr 1060/2009 och (EU) nr 648/2012[22]
Referensvärdesförordningen	Europaparlamentets och rådets förordning (EU) 2016/1011 av den 8 juni 2016 om index som används som referensvärden för finansiella instrument och finansiella avtal eller för att mäta investeringsfonders resultat, och om ändring av direktiven 2008/48/EG och 2014/17/EU och förordning (EU) nr 596/2014[23]

[17] EUT L 87, 31.3.2017, s. 126.
[18] EUT L 257, 28.8.2014, s. 1.
[19] EUT L 65, 10.3.2017, s. 48.
[20] EUT L 302, 17.11.2009, s. 1.
[21] EUT L 140, 30.5.2012, s. 32.
[22] EUT L 347, 28.12.2017, s. 35.
[23] EUT L 171, 29.6.2016, s. 1.

Kommissionens delegerade förordning (EU) 2018/1646	Kommissionens delegerade förordning (EU) 2018/1646 av den 13 juli 2018 om komplettering av Europaparlamentets och rådets förordning (EU) 2016/1011 vad gäller tekniska tillsynsstandarder för den information som ska lämnas i ansökan om auktorisation och i ansökan om registrering[24]
Dataskyddsförordningen	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)[25]

Förkortningar

Esma	Europeiska värdepappers- och marknadsmyndigheten
EU	Europeiska unionen

Definitioner

funktion	Alla processer, tjänster eller aktiviteter.
kritisk eller viktig funktion	När ett fel eller en brist i funktionens utförande allvarligt skulle försämra a) ett företags uppfyllande av sina skyldigheter enligt tillämplig lagstiftning, b) ett företags finansiella resultat, eller c) sundheten eller kontinuiteten i ett företags huvudsakliga tjänster och verksamheter.
molntjänster	Tjänster som tillhandahålls med hjälp av molnbaserade datortjänster.
molnbaserade datortjänster eller moln[26]	En modell som möjliggör nätverkstillgång till ett antal delade datorresurser (t.ex. servrar, operativsystem, nätverk, programvara, applikationer och lagring) som snabbt kan tillhandahållas och levereras med självbetjäning och administration.
molntjänstleverantör	En tredje part som tillhandahåller molntjänster inom ramen för ett uppdragsavtal om molntjänster.

[24] EUT L 274, 5.11.2018, s. 43.
[25] EUT L 119, 4.5.2016, s. 1.
[26] Datormoln förkortas ofta ”moln”. Termen ”moln” används genomgående i resten av dokumentet för att underlätta hänvisningar.

uppdragsavtal om molntjänster	Alla former av avtal, inbegripet delegeringsavtal, mellan (i) ett företag och en molntjänstleverantör genom vilka denna leverantör utför en funktion som annars skulle kunna utföras av företaget självt, eller (ii) ett företag och en tredje part som inte är en molntjänstleverantör, men som har starkt beroende av att en sådan leverantör utför en funktion som annars skulle kunna utföras av företaget självt. I detta fall bör en hänvisning till en ”molntjänstleverantör” i dessa riktlinjer tolkas som en hänvisning till en sådan tredje part.
underentreprenad	En situation där en molntjänstleverantör överför en utkontrakterad funktion (eller en del av den funktionen) vidare till en annan tjänsteleverantör inom ramen för ett uppdragsavtal.
modell för molnanvändning	Det sätt på vilket molninfrastruktur kan organiseras för kontroll och användning av dataresurser. Modellerna för molnanvändning omfattar gruppmoln [27], hybridmoln [28], privat moln[29] och offentligt moln[30].
företag	a) Förvaltare av alternativa investeringsfonder eller AIF-förvaltare enligt definitionen i artikel 4.1 b i direktivet om AIF-förvaltare och förvaringsinstitut enligt artikel 21.3 i samma direktiv (nedan kallade *förvaringsinstitut för alternativa investeringsfonder (AIF-fonder)*). b) Förvaltningsbolag enligt definitionen i artikel 2.1 b i fondföretagsdirektivet (nedan kallade *förvaltningsbolag för fondföretag*) och förvaringsinstitut enligt definitionen i artikel 2.1 a i fondföretagsdirektivet (nedan kallade *förvaringsinstitut för fondföretag*). c) Centrala motparter enligt definitionen i artikel 2.1 i Emir och centrala motparter från tredjeland i den mening som avses i

[27] En modell för molnanvändning där molntjänster uteslutande är till för och delas av en viss grupp molntjänstkunder som har gemensamma krav och ett förhållande till varandra, och där resurserna kontrolleras av minst en medlem i denna grupp.
[28] En modell för molnanvändning som bygger på en kombination av minst två olika modeller för molnanvändning.
[29] En modell för molnanvändning där molntjänsterna uteslutande används av en enda molntjänstkund och där resurserna kontrolleras av den molntjänstkunden.
[30] En modell för molnanvändning där molntjänster kan vara tillgängliga för alla molntjänstkunder och där resurserna kontrolleras av molntjänstleverantören.

artikel 25.2a i Emir, vilka uppfyller tillämpliga krav enligt artikel 25.2b a i Emir.

d) Transaktionsregister enligt definitionen i artikel 2.2 i Emir och artikel 3.1 i förordningen om transparens i transaktioner för värdepappersfinansiering.

e) Värdepappersföretag enligt definitionen i artikel 4.1.1 i Mifid II och kreditinstitut enligt definitionen i artikel 4.1.27 i Mifid II för investeringstjänster och investeringsverksamhet i den mening som avses i artikel 4.1.2 i Mifid II.

f) Leverantörer av datarapporteringstjänster enligt definitionen i artikel 4.1.63 i Mifid II[31].

g) Handelsplatsers marknadsoperatörer i den mening som avses i artikel 4.1.24 i Mifid II.

h) Värdepapperscentraler enligt definitionen i artikel 2.1.1 i CSD-förordningen.

i) Kreditvärderingsinstitut enligt definitionen i artikel 3.1 b i förordningen om kreditvärderingsinstitut.

j) Värdepapperiseringsregister enligt definitionen i artikel 2.23 i förordningen om värdepapperisering.

k) Administratörer av kritiska referensvärden enligt definitionen i artikel 3.1.25 i referensvärdesförordningen.

III. Syfte

5. Dessa riktlinjer utgår från bestämmelserna i artikel 16.1 i Esmaförordningen. Syftet med dessa riktlinjer är att etablera konsekventa, effektiva och ändamålsenliga tillsynsmetoder inom det europeiska systemet för finansiell tillsyn och säkra en gemensam, enhetlig och konsekvent tillämpning av de krav som avses i avsnitt 1.1, för

[31] Från och med den 1 januari 2022 bör hänvisningen till denna bestämmelse läsas som en hänvisning till led 36a i artikel 2.1 i Mifir.

utkontraktering till molntjänstleverantörer. Dessa riktlinjer syftar särskilt till att hjälpa företag och behöriga myndigheter att identifiera, hantera och övervaka de risker och utmaningar som uppstår i samband med uppdragsavtal om molntjänster, från beslut om att lägga ut molntjänster på en leverantör, val av molntjänstleverantör och övervakning av utkontrakterad funktion till utträde ur utkontrakteringen.

IV. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

6. I enlighet med artikel 16.3 i Esmaförordningen bör de behöriga myndigheterna och företag med alla tillgängliga medel söka följa riktlinjerna.

7. Behöriga myndigheter som berörs av riktlinjerna bör efterleva dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sitt nationella rättsliga ramverk och/eller sina tillsynsrutiner), även när riktlinjer i första hand riktas till företag. I det fallet bör de behöriga myndigheterna genom sin tillsyn se till att företagen följer riktlinjerna.

8. Genom sin direkta tillsyn kommer Esma att bedöma tillämpningen av dessa riktlinjer av kreditvärderingsinstitut, transaktionsregister, värdepapperiseringsregister, centrala motparter från tredjeland och, från och med den 1 januari 2022, leverantörer av datarapporteringstjänster och administratörer av kritiska referensvärden.

Rapporteringskrav

9. Inom två månader efter det att riktlinjerna har offentliggjorts på Esmas webbplats på alla officiella EU-språk bör de behöriga myndigheterna meddela Esma om de i) följer dessa riktlinjer, eller ii) inte följer men avser att följa dessa riktlinjer, eller iii) inte följer och inte avser att följa dessa riktlinjerna.

10. Om riktlinjerna inte följs bör behöriga myndigheter inom två månader efter det att riktlinjerna har offentliggjorts på Esmas webbplats på alla officiella EU-språk meddela Esma om skälen till att de inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på Esmas webbplats. Så snart anmälningen har fyllts i ska den översändas till Esma.

11. Företag är inte skyldiga att rapportera huruvida de följer dessa riktlinjer.

V. Riktlinjer om utkontraktering till molntjänstleverantörer

Riktlinje 1. Styrning, tillsyn och dokumentation

12. Ett företag bör ha en fastställd, godkänd och aktuell strategi för uppdragsavtal om molntjänster. Strategin för uppdragsavtal om molntjänster ska stämma överens med företagets relevanta affärsstrategier och strategier för informations- och kommunikationsteknik (IKT), interna riktlinjer och riskhanteringsprocesser, inklusive hantering av IKT, informationssäkerhet och operativa risker.

13. Ett företag bör

    a) fastställa tydliga ansvarsområden för dokumentation, förvaltning och kontroll av utkontrakteringslösningarna till molntjänstleverantörer inom sin organisation,
    b) tillse att företagets personal är tillräckligt stor och kompetent för att säkerställa efterlevnaden av dessa riktlinjer och alla rättsliga krav som är tillämpliga på dess utkontrakteringslösningar till molntjänstleverantörer,
    c) upprätta en funktion för övervakning av utkontrakteringen till molntjänstleverantörer eller utse en medarbetare i högre ställning som är direkt ansvarig inför ledningsorganet och har ansvar för att förvalta och kontrollera riskerna med utkontrakteringslösningar till molntjänstleverantörer. När företagen följer dessa riktlinjer bör de ta hänsyn till verksamhetens art, omfattning och komplexitet, inbegripet i fråga om risker för det finansiella systemet, samt de inneboende riskerna med de utkontrakterade funktionerna, och se till att deras ledningsorgan har relevant teknisk kompetens för att förstå riskerna med utkontrakteringslösningarna till molntjänstleverantörer[32]. Små och mindre komplexa företag bör som minst säkerställa en tydlig uppdelning av uppgifter och ansvar för förvaltningen och kontrollen av utkontrakteringslösningarna till molntjänstleverantörer.

14. Ett företag bör övervaka molntjänstleverantörernas verksamhet, säkerhetsåtgärder och efterlevnad av överenskomna servicenivåer. Denna övervakning bör vara riskbaserad, med huvudfokus på utkontrakteringen av kritiska eller viktiga funktioner.

15. Ett företag bör regelbundet ompröva huruvida dess uppdragsavtal om molntjänster avser en kritisk eller viktig funktion, eller om risken, arten eller omfattningen av en utkontrakterad funktion har ändrats väsentligt.

16. Ett företag bör föra ett uppdaterat register med information om alla sina uppdragsavtal om molntjänster, och skilja mellan utkontraktering av kritiska eller viktiga funktioner och andra uppdragsavtal. När företaget skiljer mellan utkontraktering av kritiska eller viktiga funktioner och andra uppdragsavtal bör det ge en kort sammanfattning av skälen till att den utkontrakterade funktionen är eller inte anses vara kritisk eller viktig. Med hänsyn

[32] För värdepappersföretag och kreditinstitut, se Esmas och EBA:s gemensamma riktlinjer för lämplighetsbedömningar av ledamöter i ledningsorganet och personer som innehar nyckelfunktioner enligt direktiv 2013/36/EU och direktiv 2014/65/EU (EBA/GL/2017/12).

till nationell lagstiftning bör företaget också föra register över avslutade uppdragsavtal om molntjänster under en lämplig tid.

17. Vid uppdragsavtal om molntjänster för kritiska eller viktiga funktioner bör registret innehålla åtminstone följande information om varje uppdragsavtal:

    a) Ett referensnummer.
    b) Startdatum och, efter vad som är tillämpligt, datum för nästa kontraktsförnyelse, slutdatum och/eller uppsägningstider för molntjänstleverantören och för företaget.
    c) En kort beskrivning av den utkontrakterade funktionen, inklusive de uppgifter som utkontrakteras och huruvida dessa uppgifter inbegriper personuppgifter (t.ex. genom att ange ja eller nej i ett separat datafält).
    d) Företagets klassificering av typen av utkontrakterad funktion (t.ex. informationsteknisk (it) funktion, kontrollfunktion), i syfte att göra det lättare att identifiera olika typer av uppdragsavtal om molntjänster.
    e) Huruvida den utkontrakterade funktionen stöder affärsverksamheter som är tidsmässigt kritiska.
    f) Molntjänstleverantörens namn och eventuella varumärkesnamn, registreringslandet, organisationsnumret, identifieringskoden för juridisk person (när sådan finns), den registrerade adressen och andra relevanta kontaktuppgifter, samt namnet på leverantörens moderföretag (om sådant finns).
    g) Den lagstiftning som gäller för uppdragsavtalet om molntjänster och, i förekommande fall, valet av jurisdiktion.
    h) Typ av molntjänster och modeller för molnanvändning, och den särskilda karaktären på uppgifterna som ska lagras och platserna (dvs. länder eller regioner) där sådana uppgifter kommer att lagras.
    i) Datumet för den senaste bedömningen av om den utkontrakterade funktionen är kritisk eller viktig samt datumet för nästa planerade bedömning.
    j) Datumet för den senaste riskbedömningen/revisionen av molntjänstleverantören, tillsammans med en kort sammanfattning av de viktigaste resultaten och datum för nästa planerade riskbedömning/revision.
    k) Det enskilda eller beslutsfattande organ i företaget som godkände uppdragsavtalet om molntjänster.
    l) I tillämpliga fall namnen på eventuella underentreprenörer som en kritisk eller viktig funktion (eller väsentliga delar av den) vidareutkontrakteras till, däribland de länder där underentreprenörerna är registrerade, var tjänsten kommer att utföras och de platser (dvs. regioner eller länder) där uppgifterna kommer att lagras.
    m) Den uppskattade årliga budgeterade kostnaden för uppdragsavtalet om molntjänster.

18. När det gäller uppdragsavtal om molntjänster för icke-kritiska eller icke-viktiga funktioner bör företaget fastställa vilken information som bör ingå i registret, beroende på de inneboende riskernas art, omfattning och komplexitet.

Riktlinje 2. Analys före utkontraktering och företagsutvärdering

19. Innan ett företag ingår ett uppdragsavtal om molntjänster bör det

    a) bedöma om avtalet avser en kritisk eller viktig funktion,
    b) identifiera och bedöma alla relevanta risker med utkontrakteringslösningen,
    c) genomföra lämplig företagsutvärdering av den berörda molntjänstleverantören,
    d) identifiera och bedöma eventuella intressekonflikter som utkontrakteringen kan medföra.

20. Analysen före utkontraktering och företagsutvärderingen av den berörda molntjänstleverantören bör stå i proportion till den berörda funktionens art, omfattning och komplexitet samt de inneboende riskerna med denna funktion. Den bör åtminstone omfatta en bedömning av utkontrakteringslösningens potentiella effekter på de operativa och juridiska riskerna samt efterlevnads- och ryktesriskerna för företaget.

21. Om utkontrakteringslösningen gäller kritiska eller viktiga funktioner bör företaget också

    a) bedöma alla relevanta risker som kan uppstå till följd av uppdragsavtalet om molntjänster, inbegripet risker som är förknippade med informations- och kommunikationsteknik, informationssäkerhet, driftskontinuitet, rättsliga krav och regelefterlevnad, ryktesrisker, operativa risker och eventuella tillsynsbegränsningar för företaget som uppstår från:
        i. den valda molntjänsten och de föreslagna modellerna för molnanvändning,
        ii. migreringen och/eller genomförandet,
        iii. känsligheten hos den funktion och de relaterade uppgifter som ska utkontrakteras samt de säkerhetsåtgärder som skulle behöva vidtas,
        iv. driftskompatibiliteten mellan företagets och molntjänstleverantörens system och applikationer, dvs. deras förmåga att utbyta information och ömsesidigt använda denna information,
        v. dataportabiliteten för företagets uppgifter, vilket avser förmågan att enkelt överföra företagets uppgifter till en annan molntjänstleverantör eller tillbaka till företaget,
        vi. den politiska stabiliteten, säkerhetssituationen och rättssystemet (inbegripet de befintliga brottsbekämpningsbestämmelserna, de insolvensrättsliga bestämmelser som skulle gälla om molntjänstleverantören skulle gå i konkurs, gällande lagar om uppgiftsskydd och huruvida villkoren för överföring av personuppgifter till ett tredjeland enligt dataskyddsförordningen är uppfyllda) i de länder (inom eller utanför EU) där de utkontrakterade funktionerna skulle tillhandahållas och där de utkontrakterade uppgifterna skulle lagras, samt, vid underentreprenad, de ytterligare risker som kan uppstå om underleverantören är baserad i ett tredjeland eller ett annat land än molntjänstleverantören och, i händelse av en underentreprenörskedja, eventuella ytterligare risker som kan uppstå, inbegripet i samband med avsaknaden av ett direkt avtal mellan företaget och den underleverantör som utför den utkontrakterade funktionen,
        vii. företagets övergripande koncentrationsrisk (i tillämpliga fall även på koncernnivå) på grund av att flera uppdragsavtal om molntjänster har

ingåtts med samma molntjänstleverantör samt eventuell koncentration inom EU:s finansiella sektor, på grund av att flera företag använder samma molntjänstleverantör eller en liten grupp molntjänstleverantörer. Vid bedömningen av koncentrationsrisken bör företaget beakta alla uppdragsavtal om molntjänster (och, i tillämpliga fall, uppdragsavtal om molntjänster på koncernnivå) med den molntjänstleverantören,

b) beakta uppdragsavtalets förväntade fördelar och kostnader, och samtidigt väga större risker som kan begränsas eller hanteras bättre mot de ökade risker som kan uppstå till följd av uppdragsavtalet.

22. Vid utkontraktering av kritiska eller viktiga funktioner bör företagsutvärderingen omfatta en utvärdering av molntjänstleverantörens lämplighet. När företaget bedömer molntjänstleverantörens lämplighet bör det se till att molntjänstleverantören har affärsmässigt rykte, lämpliga och tillräckliga förmågor, expertis, resurser (bl.a. mänskliga, informationstekniska och ekonomiska resurser), organisationsstruktur och, i tillämpliga fall, de lagstadgade auktorisationer eller registreringar som krävs för att utföra den kritiska eller viktiga funktionen på ett tillförlitligt och professionellt sätt så den kan uppfylla sina skyldigheter under den tid uppdragsavtalet om molntjänster gäller. Ytterligare faktorer att ta hänsyn till vid företagsutvärdering av molntjänstleverantören är bland annat

a) hanteringen av informationssäkerhet, särskilt skyddet av personuppgifter, konfidentiella uppgifter eller andra känsliga uppgifter,
b) servicestödet, däribland stödplaner och kontakter, och rutiner för incidenthantering, och
c) kontinuitets- och katastrofplanerna.

23. Om så är lämpligt, och för att underlätta företagsutvärderingen, kan företaget också använda certifieringar baserade på internationella standarder och externa eller interna revisionsrapporter.

24. Om företaget får kännedom om stora brister och/eller betydande förändringar i de tjänster som tillhandahålls eller i molntjänstleverantörens situation bör analysen före utkontrakteringen och företagsutvärderingen av molntjänstleverantören snarast ses över eller göras om.

25. Om företaget ingår ett nytt avtal eller förnyar ett befintligt avtal med en molntjänstleverantör som redan har utvärderats, bör företaget genom en riskbaserad metod fastställa om det krävs en ny företagsutvärdering.

Riktlinje 3. Viktiga delar av avtalet

26. Ett företags och dess molntjänstleverantörs rättigheter och skyldigheter bör klart och tydligt anges i ett skriftligt avtal.

27. Det skriftliga avtalet bör uttryckligen ge företaget möjlighet att säga upp det.

28. Vid utkontraktering av kritiska eller viktiga funktioner bör det skriftliga avtalet åtminstone innehålla följande:

    a) En tydlig beskrivning av den utkontrakterade funktionen.

    b) Startdatum och slutdatum, i tillämpliga fall, för avtalet samt uppsägningstiderna för molntjänstleverantören och företaget.

    c) Tillämplig lag för avtalet och, i förekommande fall, valet av jurisdiktion.

    d) Företagets och molntjänstleverantörens finansiella skyldigheter.

    e) Huruvida underentreprenad är tillåten och, om så är fallet, på vilka villkor, med beaktande av riktlinje 7.

    f) Platsen/platserna (dvs. regioner eller länder) där den utkontrakterade funktionen kommer att tillhandahållas och där data kommer att behandlas och lagras, samt de villkor som ska vara uppfyllda, inbegripet kravet att företaget ska meddelas om molntjänstleverantören vill ändra platsen eller platserna.

    g) Bestämmelser om informationssäkerhet och skydd av personuppgifter, med beaktande av riktlinje 4.

    h) Företagets rätt att regelbundet övervaka molntjänstleverantörens fullgörande av uppdragsavtalet om molntjänster, med beaktande av riktlinje 6.

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

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

    k) Bestämmelser om molntjänstleverantörens hantering av incidenter, inbegripet skyldigheten att utan onödigt dröjsmål rapportera incidenter som har påverkat företagets avtalade tjänster.

    l) Huruvida molntjänstleverantören bör teckna en obligatorisk försäkring mot vissa risker och, i tillämpliga fall, nivån på det begärda försäkringsskyddet.

    m) Kraven att molntjänstleverantören ska införa och testa kontinuitets- och katastrofplaner.

    n) Kravet att molntjänstleverantören ska ge företaget, behöriga myndigheter och andra personer som utsetts av företaget eller de behöriga myndigheterna rätt att få tillgång till (nedan kallad *rätt till tillträde*) och granska (nedan kallad *rätt till revision*) molntjänstleverantörens relevanta information, lokaler, system och utrustning i den utsträckning det är nödvändigt för att övervaka molntjänstleverantörens resultat enligt överenskommelsen om uppdragsavtal om molntjänster samt säkerställa molntjänstleverantörens efterlevnad av tillämpliga lagstadgade och avtalsenliga krav, med beaktande av riktlinje 6.

o) Bestämmelser som säkerställer att de uppgifter som molntjänstleverantören behandlar eller lagrar för företagets räkning vid behov kan nås, hämtas och återlämnas till företaget, med beaktande av riktlinje 5.

Riktlinje 4. Informationssäkerhet

29. Ett företag bör fastställa informationssäkerhetskrav i sina interna policyer och rutiner och inom ramen för det skriftliga uppdragsavtalet om molntjänster samt fortlöpande övervaka efterlevnaden av dessa krav, bland annat för att skydda konfidentiella, personliga eller på annat sätt känsliga uppgifter. Dessa krav bör stå i proportion till den berörda funktionens art, omfattning och komplexitet samt de inneboende riskerna med denna funktion.

30. Vid utkontraktering av kritiska eller viktiga funktioner, och utan att det påverkar tillämpningen av dataskyddsförordningens krav, bör ett företag som tillämpar en riskbaserad metod i detta syfte åtminstone

a) *informationssäkerhetens organisation:* se till att uppgifter och ansvarsområden som rör informationssäkerhet tydligt delas upp mellan företaget och molntjänstleverantören, bl.a. när det gäller identifiering av hot, sårbarheter, incidenthantering och säkerhetsuppdateringar, och se till att molntjänstleverantören kan fullgöra sina roller och skyldigheter,
b) *identitets- och åtkomsthantering:* se till att det finns starka autentiseringsmekanismer (t.ex. flerfaktorsautentisering) och åtkomstkontroller för att förhindra obehörig åtkomst till företagets data och grundsystem,
c) *kryptering och nyckelhantering:* se till att relevant krypteringsteknik vid behov används för data som överförs, data i minne, data i vila och säkerhetskopierade data, i kombination med lämpliga nyckelhanteringslösningar för att begränsa risken för obehörig åtkomst till krypteringsnycklar, och företaget bör särskilt överväga att använda den senaste tekniken och metoderna för sin nyckelhanteringslösning,
d) *drift- och nätsäkerhet:* överväga lämpliga nivåer av nättillgänglighet, nätverkssegmentering (t.ex. isolering av användare i molnets gemensamma miljö, operativ separering av webben, applikationslogik, operativsystem, nätverk, databashanterare (DBMS) och lagringsskikt) och olika IKT-miljöer (t.ex. test, utveckling, produktion),
e) *applikationsprogrammeringsgränssnitt (API):* överväga mekanismer för integrering av molntjänsterna med företagets system så att API:er blir säkra (t.ex. genom att införa och följa policyer och rutiner för informationssäkerhet i API:er som omfattar flera systemgränssnitt, jurisdiktioner och affärsfunktioner, för att förhindra att uppgifter röjs, ändras eller förstörs utan tillstånd),
f) *driftskontinuitet och katastrofberedskap:* se till att det finns effektiva kontroller av driftskontinuiteten och katastrofberedskapen (t.ex. genom att fastställa minimikrav på kapacitet, välja geografiskt spridda värdtjänster (*hosting*), så att man kan växla mellan dem, eller begära och granska dokumentation som visar hur företagets uppgifter överförs i molntjänstleverantörens system, samt överväga möjligheten att kopiera avbilder från virtuella datorer (*VMI*) till en oberoende lagringsplats som är tillräckligt isolerad från nätverket eller ligger utanför nätverket),

g) *uppgifternas lokalisering:* införa en riskbaserad metod för platser för lagring och hantering av uppgifter (dvs. regioner eller länder),
h) *efterlevnad och övervakning:* kontrollera att molntjänstleverantören uppfyller internationellt erkända standarder för informationssäkerhet och har infört lämpliga kontroller av informationssäkerheten (t.ex. genom att begära att molntjänstleverantören styrker att den utför relevanta kontroller av informationssäkerheten och genom att regelbundet bedöma och testa molntjänstleverantörens informationssäkerhet).

Riktlinje 5. Utträdesstrategier

31. Vid utkontraktering av kritiska eller viktiga funktioner bör ett företag se till att det kan säga upp uppdragsavtalet om molntjänster utan onödiga störningar av verksamheten och tjänsterna, och utan att det inverkar ofördelaktigt på dess efterlevnad av tillämplig lagstiftning eller på uppgifternas konfidentialitet, integritet och tillgänglighet. För att uppnå detta bör företaget

    a) ta fram utträdesplaner som är övergripande, dokumenterade och tillräckligt testade. Dessa planer bör uppdateras vid behov, även vid ändringar av den utkontrakterade funktionen,
    b) identifiera alternativa lösningar och ta fram övergångsplaner för att flytta den utkontrakterade funktionen och uppgifterna från molntjänstleverantören och, i tillämpliga fall, eventuella underleverantörer, till alternativa molntjänstleverantörer eller återta den utkontrakterade funktionen tillbaka till företaget. Dessa lösningar bör fastställas med hänsyn till de utmaningar som kan uppstå på grund av uppgifternas lokalisering, och nödvändiga åtgärder bör vidtas för att säkerställa driftskontinuitet under övergångsfasen,
    c) se till att det skriftliga uppdragsavtalet om molntjänster omfattar en skyldighet för molntjänstleverantören att underlätta en ordnad överföring av den utkontrakterade funktionen och den tillhörande databehandlingen från molntjänstleverantören och eventuella underleverantörer till en annan molntjänstleverantör som företaget angett eller direkt till företaget, om företaget aktiverar utträdesstrategin. Skyldigheten att underlätta en ordnad överföring av den utkontrakterade funktionen och den tillhörande databehandlingen bör i förekommande fall inbegripa säker radering av uppgifter från molntjänstleverantörens och eventuella underleverantörers system.

32. När företaget utarbetar utträdesplaner och lösningar som avses i punkter a och b ovan (*utträdesstrategin*) bör företaget tänka på följande:

    a) Definiera målsättningarna i utträdesstrategin.
    b) Definiera de triggerhändelser som kan aktivera utträdesstrategin. Dessa bör åtminstone omfatta företagets eller molntjänstleverantörens uppsägning av uppdragsavtalet om molntjänster samt konkurs eller annat allvarligt upphörande av molntjänstleverantörens affärsverksamhet.

c) Utföra en verksamhetsanalys som står i proportion till den utkontrakterade funktionen, för att utröna vilka mänskliga och övriga resurser som krävs för att genomföra utträdesstrategin.
d) Tilldela roller och ansvarsområden för hantering av utträdesstrategin.
e) Testa utträdesstrategins lämplighet med hjälp av en riskbaserad metod (t.ex. genom att göra en analys av de potentiella kostnaderna, konsekvenserna, resurserna och tidseffekterna av att överföra en utkontrakterad tjänst till en annan leverantör).
f) Definiera framgångskriterier för övergången.

33. Företagets fortlöpande övervakning och tillsyn av de tjänster som molntjänstleverantören tillhandahåller inom ramen för uppdragsavtalet om molntjänster bör omfatta indikatorer för triggerhändelser som utlöser utträdesstrategin.

Riktlinje 6. Åtkomst- och revisionsrättigheter

34. Ett företag bör se till att det skriftliga uppdragsavtalet om molntjänster inte begränsar företagets och den behöriga myndighetens rätt till inspektion och revision av molntjänstleverantören samt begränsar effektiv tillsyn.

35. När företaget fastställer hur ofta och i vilken omfattning det ska utöva sina åtkomst- eller revisionsrättigheter bör företaget beakta huruvida utkontrakteringen avser en kritisk eller viktig operativ funktion, riskernas art och omfattning samt påverkan på företaget genom utkontrakteringslösningar till molntjänster.

36. Om utövande av åtkomst- eller revisionsrättigheter, eller användningen av vissa revisionsmetoder, skapar en risk för molntjänstleverantörens miljö och/eller en annan molntjänstleverantörs kund (t.ex. genom att påverka servicenivåer, uppgifters konfidentialitet, integritets- och tillgångsaspekter), bör molntjänstleverantören ge företaget en tydlig motivering till varför detta skulle skapa en risk och komma överens med företaget om alternativa sätt att uppnå ett liknande resultat (t.ex. genom att särskilda kontroller testas i molntjänstleverantörens rapporter/certifieringar).

37. Utan att det påverkar företagets slutliga ansvar för de verksamheter som utförs av molntjänstleverantörerna kan företaget, i syfte att använda revisionsresurserna på ett effektivare sätt och minska den organisatoriska bördan för molntjänstleverantören och dess kunder, använda

a) tredjepartscertifieringar och externa eller interna revisionsrapporter som har gjorts tillgängliga av molntjänstleverantören,
b) gemensamma revisioner som utförs tillsammans med andra av molntjänsteleverantörens kunder eller gemensamma revisioner som utförs av en tredje part revisor som utsetts av flera kunder till samma molntjänstleverantör.

38. Vid utkontraktering av kritiska eller viktiga funktioner bör företaget bedöma huruvida de tredjepartscertifieringar och externa eller interna revisionsrapporter som avses i punkt

37(a) är adekvata och tillräckliga för att uppfylla deras lagstadgade skyldigheter, och bör med tiden sträva efter att inte enbart förlita sig på dessa certifieringar och rapporter.

39. Vid utkontraktering av kritiska eller viktiga funktioner bör företaget använda sig av de tredjepartscertifieringar och externa eller interna revisionsrapporter som avses i punkt 37(a) endast om företaget

    a) är helt säkert på att certifieringarna eller revisionsrapporterna avser molntjänstleverantörens viktiga system (t.ex. processer, applikationer, infrastruktur, datacenter), de viktiga kontroller som identifierats av företaget samt efterlevnad av relevanta regleringskrav,
    b) noggrant och regelbundet bedömer innehållet i certifieringarna eller revisionsrapporterna och kontrollerar att certifieringarna eller rapporterna inte är inaktuella,
    c) säkerställer att molntjänstleverantörens centrala system och kontroller omfattas av framtida versioner av certifieringar eller revisionsrapporter,
    d) är tillfreds med den certifierande eller granskande partens lämplighet (t.ex. när det gäller kvalifikationer, sakkunskap, upprepning/verifiering av bevisen i den underliggande revisionsdokumentationen samt rotation av certifierings- eller revisionsföretag),
    e) är tillfreds med att certifieringarna och revisionerna utförs på grundval av lämpliga standarder och omfattar ett test av den operativa effektiviteten hos de centrala kontroller som har införts,
    f) har den avtalsmässiga rätten att begära att certifieringarnas eller revisionsrapporternas omfattning utökas till molntjänstleverantörens 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 avtalsmässiga rätten att efter eget godtycke utföra enskilda revisioner på plats med avseende på den utkontrakterade funktionen.

40. Innan ett planerat besök på plats äger rum, inbegripet av en tredje part som utsetts av företaget (t.ex. en revisor), bör företaget skäligen meddela detta till molntjänstleverantören, tillräckligt långt i förväg, såvida inte detta är omöjligt på grund av en nöd- eller krissituation eller skulle leda till att revisionen inte längre är ändamålsenlig. Ett sådant meddelande bör omfatta uppgifter om platsen för besöket, syfte samt den personal som kommer att närvara vid besöket.

41. Med tanke på att molntjänster är tekniskt komplexa och medför särskilda jurisdiktionsmässiga utmaningar bör den personal som utför revisionen – dvs. företagets internrevisorer eller revisorer som agerar för dess räkning – ha rätt kompetens och kunskap för att korrekt kunna bedöma de relevanta molntjänsterna och utföra en ändamålsenlig och relevant revision. Detta bör också gälla företagets personal som granskar molntjänstleverantörens certifieringar eller revisionsrapporter.

Riktlinje 7. Underentreprenad

42. Om underentreprenad tillåts för kritiska eller viktiga funktioner (eller väsentliga delar av dem) bör man i det skriftliga uppdragsavtalet om molntjänster mellan företaget och molntjänstleverantören

    a) ange vilka delar eller aspekter av den utkontrakterade funktionen som är undantagna från potentiell underentreprenad,
    b) specificera de villkor som ska efterlevas vid underentreprenad,
    c) specificera att molntjänstleverantören behåller fullt ansvar och är skyldig att kontrollera de tjänster som den har utkontrakterat, för att säkerställa att alla avtalsförpliktelser mellan molntjänstleverantören och företaget kontinuerligt uppfylls,
    d) innehålla en skyldighet för molntjänstleverantören att informera företaget om all planerad underentreprenad eller väsentliga ändringar av en sådan, särskilt om detta kan påverka molntjänstleverantörens förmåga att fullgöra sina skyldigheter enligt uppdragsavtalet om molntjänster med företaget. Anmälningsperioden som anges i det skriftliga avtalet bör ge företaget tillräckligt med tid för att åtminstone göra en riskbedömning av den föreslagna underentreprenaden eller väsentliga förändringar av denna samt invända mot förändringarna eller uttryckligen godkänna dem, i enlighet med punkt (e) nedan,
    e) säkerställa att företaget har rätt att invända mot den planerade underentreprenaden eller väsentliga förändringar av denna, eller att ett uttryckligt godkännande krävs innan den föreslagna underentreprenaden eller de väsentliga ändringarna träder i kraft,
    f) säkerställa att företaget har avtalsenlig rätt att säga upp uppdragsavtalet om molntjänster med molntjänstleverantören om det invänder mot den föreslagna underentreprenaden eller väsentliga förändringar av denna samt vid otillbörlig underentreprenad (t.ex. om molntjänstleverantören inte informerar företaget om underentreprenaden eller inte respekterar de villkor för underentreprenad som anges i uppdragsavtalet).

43. Företaget bör se till att molntjänstleverantören övervakar underentreprenören på lämpligt sätt.

Riktlinje 8. Skriftlig anmälan till behöriga myndigheter

44. Företaget bör i god tid skriftligen informera sin behöriga myndighet om planerade utkontrakteringslösningar om molntjänster som rör en kritisk eller viktig funktion. Företaget bör också i god tid och skriftligen informera sin behöriga myndighet om de utkontrakteringslösningar om molntjänster som avser en funktion som tidigare klassificerades som icke-kritisk eller icke-viktig och som därefter blev kritisk eller viktig.

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

a) Startdatum för uppdragsavtalet om molntjänster och, i tillämpliga fall, datum för nästa kontraktsförnyelse, slutdatum och/eller uppsägningstider för molntjänstleverantören och för företaget.
b) En kortfattad beskrivning av den utkontrakterade funktionen.
c) En kort sammanfattning av anledningarna till att den utkontrakterade funktionen anses vara kritisk eller viktig.
d) Molntjänstleverantörens namn och eventuella varumärkesnamn, registreringslandet, organisationsnumret, identifieringskoden för juridisk person (när sådan finns), den registrerade adressen och andra relevanta kontaktuppgifter, samt namnet på leverantörens moderföretag (om sådant finns).
e) Tillämplig lag för uppdragsavtalet om molntjänster och, i förekommande fall, valet av jurisdiktion.
f) Modellerna för molnanvändning, och den särskilda karaktären på uppgifterna som ska lagras och platserna (dvs. länder eller regioner) där sådana uppgifter kommer att lagras.
g) Datumet för den senaste bedömningen av om den utkontrakterade funktionen är kritisk eller viktig.
h) Datumet för den senaste riskbedömningen eller revisionen av molntjänstleverantören, tillsammans med en kort sammanfattning av de viktigaste resultaten och datum för nästa planerade riskbedömning eller revision.
i) Det enskilda eller beslutsfattande organ i företaget som godkände uppdragsavtalet om molntjänster.
j) I tillämpliga fall namnen på eventuella underentreprenörer som väsentliga delar av en kritisk eller viktig funktion vidareutkontrakteras till, däribland det land eller den region där underentreprenörerna är registrerade, var tjänsten kommer att utföras och där uppgifterna kommer att lagras.

Riktlinje 9. Tillsyn över utkontrakteringslösningar till molntjänster

46. Behöriga myndigheter bör som ett led i sin tillsyn analysera riskerna med företagens utkontrakteringslösningar till molntjänster. Denna bedömning bör särskilt inriktas på överenskommelser som avser utkontraktering av kritiska eller viktiga funktioner.

47. De behöriga myndigheterna bör vara helt säkra på att de kan utföra en ändamålsenlig tillsyn, särskilt när företagen utkontrakterar kritiska eller viktiga funktioner som utförs utanför EU.

48. De behöriga myndigheterna bör genom en riskbaserad metod bedöma om företagen

a) har infört relevanta styrnings-, resurs- och driftsprocesser för att på lämpligt och effektivt sätt ingå, genomföra och övervaka uppdragsavtal om molntjänster,
b) identifierar och bedömer alla relevanta risker med utkontrakteringen.

49. Om koncentrationsrisker identifieras bör de behöriga myndigheterna övervaka utvecklingen av sådana risker och utvärdera både deras potentiella inverkan på andra företag som de utövar tillsyn över och finansmarknadens stabilitet.