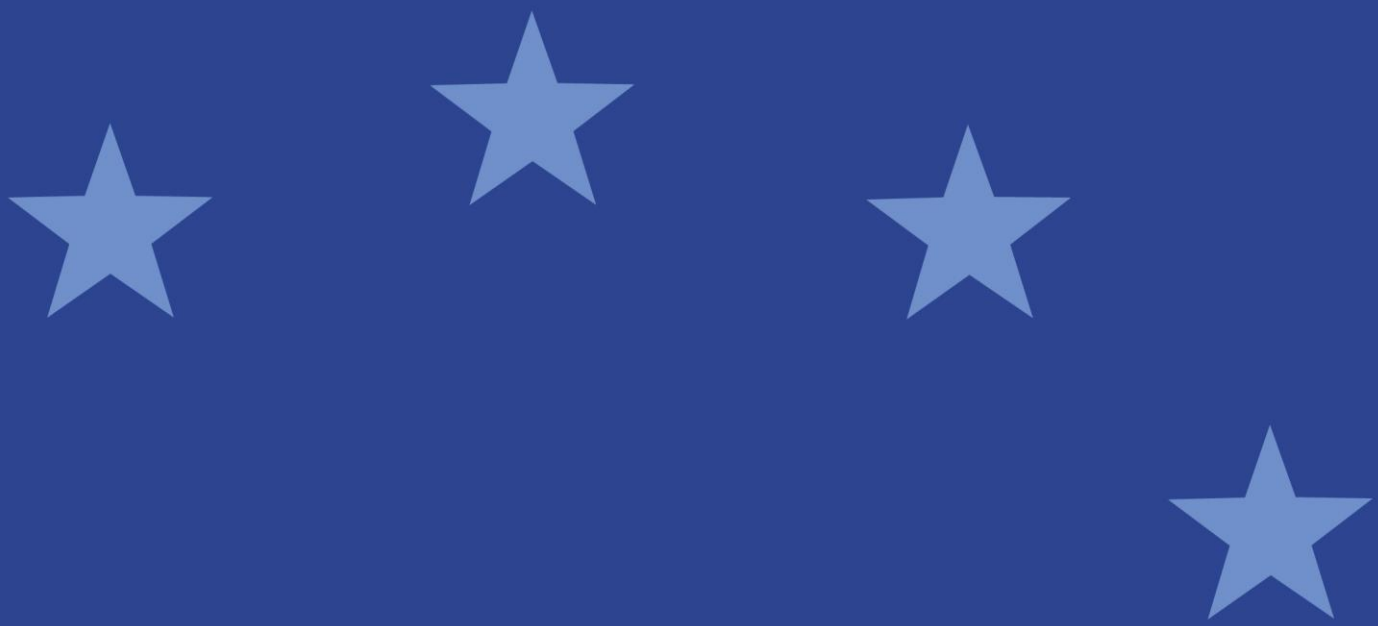
esma European Securities and Markets Authority

Retningslinjer

for outsourcing til cloududbydere



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

Indholdsfortegnelse

I. Anvendelsesområde 2
II. Henvisninger til lovgivning, forkortelser og definitioner 3
III. Formål 10
IV. Overholdelses- og rapporteringsforpligtelser 11
V. Retningslinjer for outsourcing til cloududbydere 11
Retningslinje 1. Governance, tilsyn og dokumentation 11
Retningslinje 2. Analyse og due diligence inden outsourcing 13
Retningslinje 3. Centrale kontraktforhold 15
Retningslinje 4. Informationssikkerhed 17
Retningslinje 5. Exitstrategier 18
Retningslinje 6. Adgangs- og revisionsrettigheder 19
Retningslinje 7. Videreoutsourcing 21
Retningslinje 8. Skriftlig underretning af kompetente myndigheder 22
Retningslinje 9. Tilsyn med cloudoutsourcingaftaler 23

I. Anvendelsesområde

Hvem?

1. Disse retningslinjer finder anvendelse på kompetente myndigheder og i) forvaltere af alternative investeringsfonde (FAIF'er) og depositarer for alternative investeringsfonde (AIF'er), ii) visse institutter for kollektiv investering i værdipapirer (UCITS), administrationsselskaber og depositarer for UCITS-institutter, og investeringsselskaber, der ikke har udpeget et administrationsselskab godkendt i overensstemmelse med UCITS-direktivet, iii) centrale modparter (CCP'er), herunder tredjelands-niveau 2-CCP'er, der opfylder de relevante EMIR-krav, iv) transaktionsregistre, v) investeringsselskaber og kreditinstitutter, når de udfører investeringstjenester og -aktiviteter, udbydere af dataindberetningstjenester og markedsoperatører, der driver markedspladser, vi) værdipapircentraler (CSD'er), vii) kreditvurderingsbureauer, viii) securitiseringsregistre og ix) administratorer af kritiske benchmarks.

2. ESMA tager også disse retningslinjer i betragtning ved vurderingen af, i hvilket omfang en tredjelands-niveau 2-CCP's overholdelse af de relevante EMIR-krav er opfyldt med dens overholdelse af sammenlignelige krav i tredjelandet i henhold til artikel 25, stk. 2b, litra a), i EMIR.

Hvad?

3. Disse retningslinjer finder anvendelse, for så vidt angår følgende bestemmelser:

   a) Artikel 15, 18 og 20 og artikel 21, stk. 8, i FAIF-direktivet; artikel 13, 22, 38, 39, 40, 44 og 45 og artikel 57, stk. 1, litra d), artikel 57, stk. 2, artikel 57, stk. 3, artikel 58, 75, 76, 77, 79, 81, 82 og 98 i Kommissionens delegerede forordning (EU) 2013/231
   b) Artikel 12, stk. 1, litra a), artikel 13, artikel 14, stk. 1, litra c), artikel 22, artikel 22a, artikel 23, stk. 2, artikel 30 og 31 i UCITS-direktivet; artikel 4, stk. 1 til 3, artikel 4, stk. 5, artikel 5, stk. 2, artikel 7 og 9, artikel 23, stk. 4, artikel 32, 38, 39 og 40 i Kommissionens direktiv 2010/43/EU; artikel 2, stk. 2, litra j), artikel 3, stk. 1, artikel 13, stk. 2, artikel 15, 16 og 22 i Kommissionens delegerede forordning (EU) nr. 2016/438
   c) Artikel 25, artikel 26, stk. 1, artikel 26, stk. 3, artikel 26, stk. 6, artikel 34, 35 og 78-81 i EMIR; artikel 5 og 12 i forordningen om værdipapirfinansieringstransaktioner; artikel 3, stk. 1, litra f), artikel 3, stk. 2, artikel 4, artikel 7, stk. 2, litra d) og f), artikel 9 og 17 i Kommissionens delegerede forordning (EU) nr. 153/2013; artikel 16 og 21 i Kommissionens delegerede forordning (EU) nr. 150/2013; artikel 16 og 21 i Kommissionens delegerede forordning (EU) 2019/359
   d) Artikel 16, stk. 2, artikel 16, stk. 4, artikel 16, stk. 5, artikel 18, stk. 1, artikel 19, stk. 3, litra a), artikel 47, stk. 1), litra b) og c), artikel 48, stk. 1, artikel 64, stk. 4, artikel

65, stk. 5, og artikel 66, stk. 3,[1] i MiFID II; artikel 21, stk. 1 til 3, artikel 23, artikel 29, stk. 5, artikel 30, 31 og 32 i Kommissionens delegerede forordning (EU) nr. 2017/565; artikel 6 og 15 og artikel 16, stk. 6, i Kommissionens delegerede forordning (EU) nr. 2017/584; artikel 6, 7, 8 og 9 i Kommissionens delegerede forordning (EU) nr. 2017/571

e) Artikel 22, 26, 30, 42, 44 og 45 i CSD-forordningen og artikel 33, 47, artikel 50, stk. 1, artikel 57, stk. 2, litra i), artikel 66, 68, 75, 76, 78 og 80 i Kommissionens delegerede forordning (EU) nr. 2017/392
f) Artikel 9 og bilag I, afdeling A, punkt 4 og 8, og bilag II, punkt 17, i forordningen om kreditvurderingsbureauer og artikel 11 og 25 i Kommissionens delegerede forordning (EU) nr. 2012/449
g) Artikel 10, stk. 2, i securitiseringsforordningen
h) Artikel 6, stk. 3, og artikel 10 i benchmarkforordningen og punkt 7 i bilag I til Kommissionens delegerede forordning (EU) 2018/1646.

Hvornår?

4. Disse retningslinjer finder anvendelse fra den 31. juli 2021 på alle cloudoutsourcingaftaler, der indgås, forlænges eller ændres på eller efter denne dato. Virksomheder bør revurdere og i givet fald ændre eksisterende cloudoutsourcingaftaler med henblik på at sikre, at de tager højde for disse retningslinjer inden den 31. december 2022. Hvis en virksomhed ikke har afsluttet revurderingen af cloudoutsourcingaftaler for kritiske eller vigtige funktioner inden den 31. december 2022, skal den underrette sin kompetente myndighed herom, herunder om, hvilke foranstaltninger der er planlagt for at afslutte revurderingen, eller den mulige exitstrategi.

II. Henvisninger til lovgivning, forkortelser og definitioner

Henvisninger til lovgivning

ESMA-forordningen	Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF[2]
FAIF-direktivet	Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt

[1] Fra den 1. januar 2022 skal henvisningen til artikel 64, stk. 4, artikel 65, stk. 5, og artikel 66, stk. 3, i MiFID II forstås som en henvisning til artikel 27g, stk. 4, artikel 27h, stk. 5, og artikel 27i, stk. 3, i MiFIR.
[2] EUT L 331 af 15.12.2010, s. 84.

	forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010[3]
Kommissionens delegerede forordning (EU) 2013/231	Kommissionens delegerede forordning (EU) nr. 2013/231 af 19. december 2012 om udbygning af Europa-Parlamentets og Rådets direktiv 2011/61/EU for så vidt angår undtagelser, generelle vilkår for drift, depositarer, gearing, gennemsigtighed og tilsyn[4]
UCITS-direktivet	Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love, forordninger og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (UCITS)[5]
Kommissionens direktiv 2010/43/EU	Kommissionens direktiv 2010/43/EU af 1. juni 2010 om gennemførelse af Europa - Parlamentets og Rådets direktiv 2009/65/EF for så vidt angår organisatoriske krav, interessekonflikter, god forretningsskik, risikostyring og indholdet af aftalen mellem en depositar og et administrationsselskab[6]
Kommissionens delegerede forordnin (EU) nr. 2016/438	Kommissionens delegerede forordning (EU) 2016/438 af 17. december 2015 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2009/65/EF for så vidt angår depositarers forpligtelser[7]
EMIR	Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre[8]
Forordningen om værdipapirfinansieringstransaktioner	Europa-Parlamentets og Rådets forordning (EU) 2015/2365 af 25. november 2015 om gennemsigtighed af værdipapirfinansieringstransaktioner og vedrørende genanvendelse samt om ændring af forordning (EU) nr. 648/2012[9]
Kommissionens delegerede forordning (EU) nr. 153/2013	Kommissionens delegerede forordning (EU) 153/2013 af 19. december 2012 om udbygning af Europa-Parlamentets og Rådets forordning (EU)

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

	nr. 648/2012 for så vidt angår reguleringsmæssige tekniske standarder for krav vedrørende centrale modparter[10]
Kommissionens delegerede forordning (EU) nr. 150/2013	Kommissionens delegerede forordning (EU) nr. 150/2013 af 19. december 2012 om udbygning af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 om OTC-derivater, centrale modparter og transaktionsregistre for så vidt angår reguleringsmæssige tekniske standarder for de oplysninger, som transaktionsregistre skal afgive ved ansøgning om registrering[11]
Kommissionens delegerede forordning (EU) 2019/359	Kommissionens delegerede forordning (EU) 2019/359 af 13. december 2018 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2015/2365 for så vidt angår reguleringsmæssige tekniske standarder, som præciserer indholdet af ansøgningen om registrering og udvidelse af registreringen som transaktionsregister[12]
MiFID II	Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU[13]
MiFIR	Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 om markeder for finansielle instrumenter og om ændring af forordning (EU) nr. 648/2012 ([14])
Kommissionens delegerede forordnin (EU) 2017/565	Kommissionens delegerede forordning (EU) 2017/565 af 25. april 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår de organisatoriske krav til og vilkårene for drift af investeringsselskaber samt definitioner af begreber med henblik på nævnte direktiv[15]
Kommissionens delegerede forordning (EU) nr. 2017/584	Kommissionens delegerede forordning (EU) 2017/584 af 14. juli 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår

[10] EUT L 52 af 23.2.2013, s. 41.
[11] EUT L 52 af 23.2.2013, s. 25.
[12] EUT L 81 af 22.3.2019, s. 45.
[13] EUT L 173 af 12.6.2014, s. 349.
[14] EUT L 173 af 12.6.2014, s. 84.
[15] EUT L 87 af 31.3.2017, s. 1.

	reguleringsmæssige tekniske standarder om præcisering af organisatoriske krav til markedspladser[16]
Kommissionens delegerede forordning (EU) nr. 2017/571	Kommissionens delegerede forordning (EU) 2017/571 af 2. juni 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår reguleringsmæssige tekniske standarder for udbydere af dataindberetningstjenester vedrørende godkendelse, organisatoriske krav og offentliggørelse af transaktioner[17]
CSD-forordningen	Forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012[18]
Kommissionens delegerede forordnin (EU) nr. 2017/392	Kommissionens delegerede forordning (EU) 2017/392 af 11. november 2016 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 for så vidt angår reguleringsmæssige tekniske standarder for krav vedrørende tilladelse, tilsyn og drift i forbindelse med værdipapircentraler[19]
Forordningen om kreditvurderingsbureauer	Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer[20]
Kommissionens delegerede forordning (EU) nr. 2012/449	Kommissionens delegerede forordning (EU) 449/2012 af 21. marts 2012 om udbygning af Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 for så vidt angår reguleringsmæssige tekniske standarder for de oplysninger, som kreditvurderingsbureauer skal indgive ved ansøgning om registrering og certificering[21]
Securitiseringsforordningen	Europa-Parlamentets og Rådets forordning (EU) 2017/2402 af 12. december 2017 om en generel ramme for securitisering og om oprettelse af en specifik ramme for simpel, transparent og

[16] EUT L 87 af 31.3.2017, s. 350.
[17] EUT L 87 af 31.3.2017, s. 126.
[18] EUT L 257 af 28.8.2014, s. 1.
[19] EUT L 65 af 10.3.2017, s. 48.
[20] EUT L 302 af 17.11.2009, s. 1.
[21] EUT L 140 af 30.5.2012, s. 32.

	standardiseret securitisering og om ændring af direktiv 2009/65/EF, 2009/138/EF og 2011/61/EU og forordning (EF) nr. 1060/2009 og (EU) nr. 648/2012[22]
Benchmarkforordningen	Europa-Parlamentets og Rådets forordning (EU) 2016/1011 af 8. juni 2016 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater, og om ændring af direktiv 2008/48/EF og 2014/17/EU samt forordning (EU) nr. 596/2014[23]
Kommissionens delegerede forordning (EU) 2018/1646	Kommissionens delegerede forordning (EU) 2018/1646 af 13. juli 2018 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2016/1011 for så vidt angår reguleringsmæssige tekniske standarder for de oplysninger, som skal indgives i en ansøgning om godkendelse og i en ansøgning om registrering[24]
GDPR	Europa-Parlamentets og Rådets forordning (EU) af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og ophævelse af direktiv 95/46/EF[25]

Forkortelser

CSP	cloududbyder
ESMA	Den Europæiske Værdipapir- og Markedstilsynsmyndighed
EU	Den Europæiske Union

Definitioner

funktion	alle processer, tjenesteydelser eller aktiviteter
kritisk eller vigtig funktion	enhver funktion, hvor en fejl eller mangel ved dens udførelse i væsentlig grad ville forringe: a) en virksomheds opfyldelse af sine forpligtelser i henhold til gældende ret

[22] EUT L 347 af 28.12.2017, s. 35.
[23] EUT L 171 af 29.6.2016, s. 1.
[24] EUT L 274 af 5.11.2018, s. 43.
[25] EUT L 119 af 4.5.2016, s. 1-88.

b) en virksomheds økonomiske resultater
c) sundheden af eller kontinuiteten i en virksomheds væsentlige tjenester og aktiviteter

cloudtjenester	tjenester leveret ved brug af cloudcomputing
cloudcomputing eller cloud[26]	et paradigme til at muliggøre netværksadgang til en skalerbar og elastisk pool af delbare fysiske eller virtuelle ressourcer (f.eks. servere, operativsystemer, netværk, software, applikationer og lagringsudstyr) med selvbetjening og on demand-administration
cloududbyder	en tredjepart, der leverer cloudtjenester i medfør af en cloudoutsourcingaftale
cloudoutsourcingaftale	en aftale af enhver art, herunder delegeringsaftaler mellem: (i) en virksomhed og en cloududbyder, ifølge hvilken cloududbyderen udfører en funktion, der ellers ville blive udført af virksomheden selv, eller (ii) en virksomhed og en tredjepart, som ikke er en cloududbyder, men som i væsentlig grad gør brug af en cloududbyder til at udføre en funktion, der ellers ville blive udført af virksomheden selv. I dette tilfælde skal en henvisning til en "cloududbyder" i disse retningslinjer forstås som en henvisning til en sådan tredjepart
videreoutsourcing	en situation, hvor cloududbyderen videreoverdrager den outsourcede funktion (eller en del af funktionen) til en anden udbyder i henhold til en outsourcingaftale
cloudimplementeringsmodel	måden, hvorpå cloud kan være organiseret på grundlag af kontrol med og deling af fysiske eller virtuelle ressourcer. Cloudimplementeringsmodeller omfatter community-clouds[27] og hybride[28], private[29] og offentlige[30] clouds

[26] Cloudcomputing forkortes ofte til "cloud". For nemheds skyld anvendes termen "cloud" i resten af dokumentet.
[27] En cloudimplementeringsmodel, hvor cloudtjenesterne udelukkende understøtter og deles af en specifik sammensætning af cloudkunder, der har fælles krav samt et indbyrdes forhold, og hvor ressourcerne styres af mindst ét medlem af denne sammensætning.
[28] En cloudimplementeringsmodel, der anvender mindst to forskellige cloudimplementeringsmodeller.
[29] En cloudimplementeringsmodel, hvor cloudtjenesterne udelukkende anvendes af én cloudkunde, og hvor ressourcerne styres af den pågældende cloudkunde.
[30] En cloudimplementeringsmodel, hvor cloudtjenesterne potentielt er til rådighed for enhver cloudkunde, og hvor ressourcerne styres af cloududbyderen.

virksomheder

a) forvaltere af alternative investeringsfonde eller "FAIF'er" som defineret i artikel 4, stk. 1, litra b), i FAIF-direktivet og depositarer som omhandlet i artikel 21, stk. 3, i FAIF-direktivet ("depositarer for alternative investeringsfonde (AIF'er)")

b) administrationsselskaber som defineret i artikel 2, stk. 1, litra b), i UCITS-direktivet ("UCITS-administrationsselskaber") og depositarer som defineret i artikel 2, stk. 1, litra a), i UCITS-direktivet ("depositarer for UCITS")

c) centrale modparter (CCP'er) som defineret i artikel 2, stk. 1, i EMIR og tredjelands-niveau 2-CCP'er som omhandlet i artikel 25, stk. 2a, i EMIR, som opfylder de relevante EMIR-krav i henhold til artikel 25, stk. 2b, litra a), i EMIR

d) transaktionsregistre som omhandlet i artikel 2, stk. 2, i EMIR og i artikel 3, stk. 1, i forordningen om værdipapirfinansieringstransaktioner

e) investeringsselskaber som defineret i artikel 4, stk. 1, litra 1), i MiFID II og kreditinstitutter som defineret i artikel 4, stk. 1, litra 27), i MiFID II, som udfører investeringstjenester og -aktiviteter som

omhandlet i artikel 4, stk. 1, litra 2), i MiFID II

f) dataindberetningstjenester som defineret i artikel 4, stk. 1, litra 63), i MiFID II[31]

g) markedsoperatører, der driver markedspladser, som omhandlet i artikel 4, stk. 1, litra 24), i MiFID II

h) værdipapircentraler (CSD'er) som defineret i artikel 2, stk. 1, litra 1), i CSD-forordningen

i) kreditvurderingsbureauer som defineret i artikel 3, stk. 1, litra b), i forordningen om kreditvurderingsbureauer

j) securitiseringsregistre som defineret i artikel 2, stk. 23, i securitiseringsforordningen

k) administratorer af kritiske benchmarks som defineret i artikel 3, stk. 1, litra 25), i benchmarkforordningen.

III. Formål

5. Disse retningslinjer er baseret på artikel 16, stk. 1, i ESMA-forordningen. Formålet med disse retningslinjer er at fastlægge et sammenhængende, formålstjenligt og effektivt tilsyn inden for Det Europæiske Finanstilsynssystem (ESFS) og sikre en fælles, ensartet og konsistent anvendelse af kravene som omhandlet i afsnit 1.1 under overskriften "Hvad?", hvor virksomheder outsourcer til cloududbydere. Disse retningslinjer skal navnlig hjælpe virksomheder og kompetente myndigheder med at identificere, behandle og overvåge de risici og udfordringer, som cloudoutsourcingaftaler indebærer, lige fra at træffe beslutning om at outsource, at vælge en cloududbyder, at overvåge outsourcede aktiviteter til at levere exitstrategier.

[31] Fra den 1. januar 2022 skal henvisningen til denne bestemmelse forstås som henvisning til punkt 36a i artikel 2, stk. 1, i MiFIR.

IV. Overholdelses- og rapporteringsforpligtelser

Status for retningslinjerne

6. I henhold til artikel 16, stk. 3, i ESMA-forordningen skal de kompetente myndigheder og virksomheder bestræbe sig mest muligt på at overholde disse retningslinjer.

7. De kompetente myndigheder, som disse retningslinjer gælder for, bør efterleve dem ved at indarbejde dem i deres nationale retlige rammer og/eller tilsynssystemer, alt efter hvad der er relevant, herunder også når særlige retningslinjer primært er rettet mod virksomheder. I dette tilfælde skal de kompetente myndigheder gennem deres tilsyn sikre, at virksomheder overholder retningslinjerne.

8. Gennem sit løbende direkte tilsyn vil ESMA vurdere, hvordan disse retningslinjer anvendes af kreditvurderingsbureauer, transaktionsregistre, securiteringsregistre, tredjelands-niveau 2-CCP'er og, fra 1. januar 2022, dataindberetningstjenester og administratorer af kritiske benchmarks i EU.

Rapporteringskrav

9. De kompetente myndigheder, som disse retningslinjer gælder for, skal senest to måneder efter datoen for offentliggørelse af retningslinjerne på ESMA's websted på alle officielle EU-sprog underrette ESMA om, hvorvidt de i) overholder, ii) ikke overholder, men agter at overholde, eller iii) ikke overholder og ikke agter at overholde retningslinjerne.

10. I tilfælde af manglende efterlevelse skal de kompetente myndigheder ligeledes underrette ESMA senest to måneder efter datoen for offentliggørelse af retningslinjerne på ESMA's websted på alle officielle EU-sprog om årsagerne til, at de ikke har efterlever retningslinjerne. Et skema til denne underretning findes på ESMA's websted. Når skemaet er udfyldt, skal det sendes til ESMA.

11. Virksomheder er ikke forpligtede til at meddele, om de efterlever retningslinjerne.

V. Retningslinjer for outsourcing til cloududbydere

Retningslinje 1. Governance, tilsyn og dokumentation

12. En virksomhed bør have en entydig og opdateret cloudoutsourcingstrategi, som er i overensstemmelse med virksomhedens relevante strategier og interne politikker og processer, herunder vedrørende informations- og kommunikationsteknologi, informationssikkerhed og styring af operationelle risici.

13. En virksomhed bør:

    a) fastlægge en entydig ansvarsfordeling med hensyn til dokumentation, forvaltning og kontrol af cloudoutsourcingaftaler inden for sin organisation
    b) allokere tilstrækkelige ressourcer til at sikre, at disse retningslinjer og alle lovkrav, der gælder for dens cloudoutsourcingaftaler, overholdes
    c) etablere en tilsynsfunktion for cloudoutsourcingen eller udpege overordnede medarbejdere til at være direkte ansvarlige over for ledelsesorganet og ansvarlige for at styre og overvåge risiciene i forbindelse med cloudoutsourcingaftaler. For at overholde denne retningslinje bør virksomheder tage højde for karakteren, omfanget og kompleksiteten af deres forretning, herunder hvad angår risikoen for det finansielle system, og de risici, der er forbundet med de outsourcede funktioner, og sikre, at deres ledelsesorgan har de relevante tekniske kompetencer til at forstå de risici, der er forbundet med cloudoutsourcingaftaler[32]. Små og mindre komplekse virksomheder bør som minimum sikre en klar opgave- og ansvarsfordeling for forvaltning af og kontrol med cloudoutsourcingaftaler.

14. En virksomhed bør overvåge udførelsen af aktiviteter, sikkerhedsforanstaltningerne, og at dets cloududbydere overholder de aftalte serviceniveauer. Denne overvågning bør være risikobaseret, med et primært fokus på de kritiske eller vigtige funktioner, der er blevet outsourcet.

15. En virksomhed bør revurdere, om dens cloudoutsourcingaftaler vedrører en kritisk eller vigtig funktion på tilbagevendende grundlag, og når en outsourcet funktions risiko, karakter eller omfang har ændret sig væsentligt.

16. En virksomhed bør føre et opdateret register over oplysninger om alle sine cloudoutsourcingaftaler, hvori der skelnes mellem outsourcing af kritiske eller vigtige funktioner og andre outsourcingaftaler. Når virksomheden skelner mellem outsourcing af kritiske eller vigtige funktioner og andre outsourcingaftaler, bør den kort redegøre for årsagerne til, at den outsourcede funktion anses eller ikke anses for at være kritisk eller vigtig. Af hensyn til overholdelse af national lovgivning bør en virksomhed også føre et register over ophørte cloudoutsourcingaftaler for en relevant periode.

17. Hvad angår cloudoutsourcingaftaler vedrørende kritiske eller vigtige funktioner, bør registret som minimum indeholde følgende oplysninger om den enkelte cloudoutsourcingaftale:

    a) et referencenummer
    b) startdatoen og, hvis relevant, datoen for næste kontraktforlængelse, slutdatoen og/eller opsigelsesvarsler for cloududbyderen og for virksomheden
    c) en kort beskrivelse af den outsourcede funktion, herunder de data, der er outsourcet, og hvorvidt disse data omfatter personoplysninger (f.eks. ved at angive ja eller nej i et særskilt datafelt)

[32] Investeringsselskaber og kreditinstitutter henvises til "Fælles ESMA- og EBA-retningslinjer for vurdering af egnetheden af medlemmer af ledelsesorganet og personer med nøglefunktioner i henhold til direktiv 2013/36/EU og direktiv 2014/65/EU (EBA/GL/2017/12).

d) en kategori tildelt af virksomheden, der afspejler den outsourcede funktions karakter (f.eks. informationsteknologifunktion eller kontrolfunktion), hvilket bør gøre det muligt at identificere de forskellige typer cloudoutsourcingaftaler
e) om den outsourcede funktion understøtter tidskritiske forretningsaktiviteter
f) cloududbyderens navn og handelsnavn (hvis et sådant findes), cloududbyderens registreringsland og registreringsnummer, cloududbyderens identifikator for juridisk enhed (hvis en sådan foreligger), cloududbyderens registrerede adresse og andre relevante kontaktoplysninger samt navnet på moderselskabet (hvis et sådant findes)
g) lovvalg for cloudoutsourcingaftalen og, hvis et sådant findes, værneting
h) typen af cloudtjenester og implementeringsmodeller og den specifikke karakter af de data, der outsources, og de steder (navnlig regioner eller lande), hvor disse data kan blive opbevaret
i) datoen for den seneste vurdering af, om den outsourcede funktion er kritisk eller vigtig samt datoen for den næste planlagte vurdering
j) datoen for den seneste risikovurdering/revision af cloududbyderen sammen med en kort redegørelse for de væsentligste resultater, samt datoen for den næste planlagte risikovurdering/revision
k) den person eller det beslutningstagende organ i virksomheden, der har godkendt cloudoutsourcingaftalen
l) hvis relevant, navnene på enhver, som en kritisk eller vigtig funktion (eller væsentlige dele heraf) videreoutsources til, herunder de lande, hvor de, der videreoutsources til, er registreret, de lande, hvor den videreoutsourcede tjeneste vil blive udført, og, de steder (navnlig regioner eller lande), hvor dataene skal opbevares
m) de anslåede årlige budgetomkostninger ved cloudoutsourcingaftalen.

18. Hvad angår de cloudoutsourcingaftaler, der vedrører ikkekritiske eller ikkevigtige funktioner, bør virksomheden fastlægge, hvilke oplysninger der skal indgå i registret baseret på karakteren, omfanget og kompleksiteten af de risici, der er forbundet med den outsourcede funktion.

Retningslinje 2. Analyse og due diligence inden outsourcing

19. En virksomhed bør, inden den indgår en cloudoutsourcingaftale:

a) vurdere, om cloudoutsourcingaftalen vedrører en kritisk eller vigtig funktion
b) identificere og vurdere alle relevante risici ved cloudoutsourcingaftalen
c) gennemføre relevant due diligence vedrørende den potentielle cloududbyder
d) identificere og vurdere eventuelle interessekonflikter, som outsourcingen kan forårsage.

20. Den analyse og due diligence, der gennemføres vedrørende den potentielle cloududbyder inden outsourcing, bør stå i et rimeligt forhold til karakteren, omfanget og kompleksiteten af den funktion, som virksomheden har til hensigt at outsource, og de risici, der er forbundet med denne funktion. De bør som minimum omfatte en vurdering

af cloudoutsourcingaftalens potentielle konsekvenser for virksomhedens juridiske risici samt risici relateret til drift, overholdelse og renommé.

21. Hvis cloudoutsourcingaftalen vedrører kritiske eller vigtige funktioner, bør en virksomhed desuden:

    a) vurdere alle relevante risici, der kan opstå som følge af cloudoutsourcingaftalen, herunder risici vedrørende informations- og kommunikationsteknologi, informationssikkerhed, forretningskontinuitet, juridiske forhold og overholdelse, renommé, drift og eventuelle begrænsninger i tilsynet med virksomheden som følge af
        i. den valgte cloudtjeneste og de påtænkte implementeringsmodeller
        ii. migrations- og/eller implementeringsprocesserne
        iii. følsomheden af funktionen og de dermed forbundne data, som det overvejes at outsource, og de sikkerhedsforanstaltninger, der vil skulle iværksættes
        iv. interoperabiliteten af virksomhedens og cloududbyderens systemer og applikationer, navnlig disses evne til at udveksle oplysninger og gensidigt bruge de oplysninger, der er blevet udvekslet
        v. portabiliteten af virksomhedens data, navnlig evnen til nemt at overføre virksomhedens data fra én cloududbyder til en anden og tilbage til virksomheden
        vi. den politiske stabilitet, sikkerhedssituationen og det juridiske system (herunder de retshåndhævende bestemmelser, der er etableret, de insolvenslovgivningsbestemmelser, der ville gælde i tilfælde af cloududbyderens konkurs, den gældende lovgivning om databeskyttelse, og hvorvidt betingelserne for overførsel af personoplysninger til et tredjeland i henhold til GDPR er overholdt) i de lande (i eller uden for EU), hvor de outsourcede funktioner ville skulle leveres, og hvor de outsourcede data ville skulle opbevares; ved videreoutsourcing, de yderligere risici, der kan opstå, hvis den, der videreoutsources til, er etableret i et tredjeland eller et andet land end cloududbyderens, og, i tilfælde af en videreoutsourcingkæde, enhver yderligere risiko, der kan opstå, herunder i forbindelse med fraværet af en direkte kontrakt mellem virksomheden og den, der er videreoutsourcet til, som udfører den outsourcede funktion
        vii. en mulig koncentration inden for virksomheden (herunder, hvis relevant, på koncernniveau) som følge af flere cloudoutsourcingaftaler med den samme cloududbyder samt en mulig koncentration inden for EU's finansielle sektor, som følge af at flere virksomheder gør brug af den samme cloududbyder eller en lille gruppe cloududbydere. Ved vurderingen af koncentrationsrisikoen bør virksomheden tage alle sine cloudoutsourcingaftaler med den pågældende cloududbyder i betragtning (og, hvis relevant, cloudoutsourcingaftalerne på sit koncernniveau)

    b) tage de forventede fordele og omkostninger ved cloudoutsourcingaftalen i betragtning, herunder afveje eventuelle væsentlige risici, der kan reduceres eller

styres bedre i forhold til eventuelle væsentlige risici, der kan opstå som følge af cloudoutsourcingaftalen.

22. Ved outsourcing af kritiske eller vigtige funktioner bør due diligence indbefatte en vurdering af cloududbyderens egnethed. Ved vurderingen af cloududbyderens egnethed bør en virksomhed sikre, at cloududbyderen har det renommé, de kompetencer, de ressourcer (herunder menneskelige, IT-mæssige og økonomiske), den organisationsstruktur og, hvis relevant, de(n) relevante godkendelse(r) eller registrering(er), der er nødvendig(e) for at udføre den kritiske eller vigtige funktion på en pålidelig og professionel måde og for at opfylde sine forpligtelser i cloudoutsourcingsaftalens løbetid. Yderligere faktorer, der bør tages i betragtning i forbindelse med due diligence vedrørende cloududbyderen, omfatter, men er ikke begrænset til:

    a) håndtering af informationssikkerhed og navnlig beskyttelse af personoplysninger og fortrolige og på anden måde følsomme oplysninger
    b) supporttjenesten, herunder supportplaner og -kontakter, og processer for håndtering af hændelser
    c) forretningskontinuitet og katastrofeberedskabsplaner.

23. I det omfang det er relevant, og for at understøtte den udførte due diligence, kan en virksomhed også anvende certificeringer på grundlag af internationale standarder samt eksterne eller interne revisionsrapporter.

24. Hvis en virksomhed bliver opmærksom på betydelige mangler og/eller betydelige ændringer i de leverede tjenester eller i cloududbyderens forhold, bør den analyse og due diligence vedrørende cloududbyderen, der finder sted inden outsourcingen, straks revurderes eller om nødvendigt gentages.

25. Hvis en virksomhed indgår en ny aftale eller forlænger en eksisterende aftale med en cloududbyder, der allerede er blevet vurderet, bør selskabet på grundlag af en risikobaseret tilgang vurdere, om der er behov for en ny due diligence.

Retningslinje 3. Centrale kontraktforhold

26. En virksomheds og dens cloududbyders respektive rettigheder og forpligtelser bør være tydeligt fastsat i en skriftlig aftale.

27. Den skriftlige aftale bør udtrykkeligt indeholde en mulighed for virksomheden for at opsige aftalen om nødvendigt.

28. Ved outsourcing af kritiske eller vigtige funktioner bør den skriftlige aftale som minimum indeholde:

    a) en klar beskrivelse af den outsourcede funktion

    b) startdatoen og, hvis relevant, slutdatoen for aftalen og opsigelsesfrister for cloududbyderen og for selskabet

c) lovvalg for aftalen og, hvis et sådant findes, værneting

d) virksomhedens og cloududbyderens økonomiske forpligtelser

e) angivelse af, om videreoutsourcing er tilladt, og i givet fald under hvilke betingelser, under henvisning til retningslinje 7

f) stedet eller stederne (navnlig regioner eller lande), hvor den outsourcede funktion vil blive leveret, og hvor data vil blive behandlet og opbevaret, og de betingelser, der skal opfyldes, herunder et krav om at underrette virksomheden, hvis cloududbyderen påtænker at ændre stedet eller stederne

g) betingelser vedrørende informationssikkerhed og beskyttelse af personoplysninger, under henvisning til retningslinje 4

h) virksomhedens ret til løbende at overvåge cloududbyderens præstation i medfør af cloudoutsourcingaftalen, under henvisning til retningslinje 6

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

j) cloududbyderens forpligtelser til at rapportere til virksomheden og, hvis relevant, sende rapporter af relevans for virksomhedens sikkerhedsfunktion og nøglefunktioner, f.eks. rapporter fra cloududbyderens interne revisionsfunktion

k) bestemmelser vedrørende håndtering af hændelser begået af cloududbyderen, herunder cloududbyderens forpligtelse til uden unødig forsinkelse at rapportere til virksomheden om hændelser, der har påvirket driften af virksomhedens i aftalen indeholdte tjenester

l) om cloududbyderen bør tegne en obligatorisk forsikring mod visse risici og, hvis relevant, omfanget af den ønskede forsikringsdækning

m) kravene til cloududbyderen om at implementere og teste forretningskontinuitet og katastrofeberedskabsplaner

n) kravet til cloududbyderen om at give virksomheden, dens kompetente myndigheder og enhver anden person, der er udpeget af virksomheden eller de kompetente myndigheder, ret til at få adgang ("adgangsrettigheder") til og undersøge ("revisionsrettigheder") cloududbyderens relevante oplysninger, lokaler, systemer og enheder i det omfang, der er nødvendigt for at overvåge cloududbyderens præstation i medfør af cloudoutsourcingaftalen og dennes overholdelse af de gældende lovkrav og kontraktlige krav, under henvisning til retningslinje 6

o) bestemmelser, der skal sikre, at de data, som cloududbyderen behandler eller opbevarer på vegne af virksomheden, kan tilgås, genetableres og tilbagesendes til virksomheden efter behov, med henvisning til retningslinje 5.

Retningslinje 4. Informationssikkerhed

29. En virksomhed bør fastsætte krav vedrørende informationssikkerhed i sine interne politikker og procedurer og i den skriftlige cloudoutsourcingaftale og løbende overvåge overholdelsen af disse krav, herunder for at beskytte personoplysninger og fortrolige og på anden måde følsomme oplysninger. Disse krav bør stå i et rimeligt forhold til karakteren, omfanget og kompleksiteten af den funktion, som virksomheden outsourcer til cloududbyderen, og de risici, der er forbundet med denne funktion.

30. Af hensyn til dette bør en virksomhed, ved outsourcing af kritiske eller vigtige funktioner og med forbehold af gældende krav i henhold til GDPR, på grundlag af en risikobaseret tilgang som minimum:

    a) *informationssikkerhedsorganisation:* sikre, at der er en klar fordeling af roller og ansvarsområder vedrørende informationssikkerhed mellem virksomheden og cloududbyderen, herunder hvad angår påvisning af trusler, håndtering af hændelser samt patch management, og sikre, at cloududbyderen reelt er i stand til at udfylde sine roller og varetage sine ansvarsområder
    b) *identitets- og adgangsstyring*: sikre, at der er etableret stærke godkendelsesmekanismer (f.eks. multifaktorgodkendelse) og adgangskontroller med henblik på at forebygge uretmæssig adgang til virksomhedens data og back-end cloudressourcer
    c) *kryptering og nøgleadministration:* sikre, at relevante krypteringsteknologier anvendes, om nødvendigt, til data under overførsel, data i hukommelsen, lagrede data og data-backups i kombination med relevante nøgleadministrationsløsninger for at begrænse risikoen for ikkeberettiget adgang til krypteringsnøglerne; virksomheden skal navnlig tage de nyeste teknologier og processer i betragtning ved valg af nøgleadministrationsløsninger
    d) *drifts- og netværkssikkerhed:* tage relevante niveauer af netværkstilgængelighed, netværkssegregering (f.eks. brugerisolering i det delte miljø i clouden, operationel adskillelse med hensyn til web, programlogik, operativsystem, netværk, Database Management System (DBMS) og lagerlag) og behandlingsmiljøer (f.eks. test, User Acceptance Testing, udvikling og produktion) i betragtning
    e) *applikationsprogrammeringsinterfaces (API):* tage mekanismer til integration af cloudtjenesterne med virksomhedens systemer i betragtning med henblik på at sikre API'ers sikkerhed (f.eks. etablering og opdatering af informationssikkerhedspolitikker og -procedurer for API'er på tværs af forskellige systeminterfaces, jurisdikitioner og forretningsfunktioner for at forebygge uberettiget videregivelse, ændring eller tilintetgørelse af data)
    f) *forretningskontinuitet og katastrofeberedskab*: sikre, at der er etableret effektive kontroller af forretningskontinuitet og katastrofeberedskab (f.eks. ved at fastsætte krav om minimumskapacitet, ved at vælge hostingløsninger, der er geografisk spredt, med mulighed for at skifte fra den ene til den anden, eller ved at anmode om eller vurdere dokumentation, der viser transportruten for virksomhedens data mellem cloududbyderens systemer, samt ved at tage muligheden for at replikere diskbilleder til en uafhængig lagerplads i betragtning, som er tilstrækkeligt isoleret fra netværket eller ikke er på netværket)

g) *dataplacering*: anlægge en risikobaseret tilgang til placeringen af datalagring og databehandling (navnlig regioner eller lande)
h) *overholdelse og overvågning*: verificere, at cloududbyderen overholder internationalt anerkendte standarder for informationssikkerhed og har implementeret relevante informationssikkerhedskontroller (f.eks. ved at anmode cloududbyderen om at fremlægge dokumentation for, at denne udfører relevante tjek af informationssikkerheden, og ved at gennemføre regelmæssige vurderinger og test af cloududbyderens informationssikkerhedsordninger).

Retningslinje 5. Exitstrategier

31. Ved outsourcing af kritiske eller vigtige funktioner bør en virksomhed sikre, at den kan udtræde af cloudoutsourcingaftalen uden unødig afbrydelse af sine forretningsaktiviteter og kundetjenester samt uden ulempe for opfyldelsen af sine forpligtelser i henhold til gældende ret og for datafortroligheden, -integriteten og -tilgængeligheden. Af hensyn til dette bør en virksomhed:

    a) udvikle exitplaner, der er grundige, dokumenterede og tilstrækkeligt testet. Disse planer bør opdateres efter behov, herunder i tilfælde af ændringer i den outsourcede funktion
    b) identificere alternative løsninger og udvikle overgangsplaner for fjernelse af den outsourcede funktion og dataene fra cloududbyderen og, hvis relevant, enhver, der videreoutsources til, og overføre dem til den anden cloududbyder som angivet af virksomheden eller direkte tilbage til virksomheden. Disse løsninger bør fastlægges ud fra de udfordringer, der kan opstå som følge af dataenes placering, og med anvendelse af de nødvendige foranstaltninger til at sikre forretningskontinuitet i overgangsfasen
    c) sikre, at den skriftlige cloudoutsourcingaftale indeholder en forpligtelse for cloududbyderen til at understøtte struktureret overførsel af den outsourcede funktion, og den dermed forbundne behandling af data, fra cloududbyderen og enhver, der videreoutsources til, til en anden cloududbyder som angivet af virksomheden eller direkte til virksomheden, i tilfælde af at virksomheden aktiverer exitstrategien. Forpligtelsen til at understøtte struktureret overførsel af den outsourcede funktion, og den dermed forbundne behandling af data, bør, hvis relevant, også omfatte sikker sletning af dataene fra cloududbyderens systemer og systemerne hos enhver, der videreoutsources til.

32. Ved udvikling af exitplanerne og de løsninger, der henvises til i punkt a) og b) ovenfor ("exitstrategi"), bør virksomheder tage følgende i betragtning:

    a) definere målene for exitstrategien
    b) definere de triggerhændelser, der ville kunne aktivere exitstrategien. Disse bør som minimum omfatte ophør af cloudoutsourcingaftalen på virksomhedens eller cloududbyderens initiativ samt svigt i eller anden alvorlig indstilling af cloududbyderens forretningsaktivitet

c) udføre en konsekvensanalyse, der står i rimeligt forhold til den outsourcede funktion, for at fastlægge, hvilke menneskelige og andre ressourcer der vil være påkrævet for at gennemføre exitplanen
d) tildele roller og ansvarsområder for at håndtere exitstrategien
e) teste exitstrategiens egnethed, på grundlag af en risikobaseret tilgang (f.eks. ved at gennemføre en analyse af de potentielle omkostninger, konsekvenser, ressourcer og tidsmæssige følger af at overføre en outsourcet tjeneste til en anden udbyder)
f) fastlægge succeskriterier for overgangen.

33. En virksomhed bør inkludere indikatorer for exitstrategiens trigger-hændelser i sin løbende overvågning og sit løbende tilsyn med cloududbyderens tjenester leveret i medfør af cloudoutsourcingaftalen.

Retningslinje 6. Adgangs- og revisionsrettigheder

34. En virksomhed bør sikre, at den skriftlige cloudoutsourcingaftale ikke begrænser virksomhedens og den kompetente myndigheds reelle udøvelse af adgangs- og revisionsrettigheder og tilsynsmuligheder i forhold til cloududbyderen.

35. En virksomhed bør sikre, at udøvelsen af adgangs- og revisionsrettigheder (f.eks. revisionshyppigheden og de områder og tjenester, der skal revideres) tager i betragtning, om outsourcingen vedrører en kritisk eller vigtig funktion, samt karakteren og omfanget af risiciene og konsekvenserne i forbindelse med cloudoutsourcingaftalen for virksomheden.

36. Hvis udøvelsen af adgangs- eller revisionsrettigheder eller brugen af visse revisionsteknikker indebærer en risiko for cloududbyderens og/eller en anden af cloududbyderens kunders miljø (f.eks. ved at påvirke serviceniveauer, datafortrolighed, -integritet og -tilgængelighed), bør cloududbyderen redegøre klart over for virksomheden for, hvorfor dette indebærer en risiko, og cloududbyderen bør træffe aftale med virksomheden om alternative måder at opnå et lignende resultat på (f.eks. inkludering af specifikke kontroller, der skal testes i en specifik rapport/certificering udarbejdet af CSP).

37. Med forbehold af deres endelige ansvar for cloudoutsourcingaftaler, kan virksomheder, for at udnytte revisionsressourcerne mere effektivt og mindske den organisatoriske byrde for cloududbyderen og dennes kunder, anvende følgende:

a) tredjepartscertificeringer og eksterne eller interne revisionsrapporter, der stilles til rådighed af cloududbyderen
b) samlede revisioner udført sammen med andre af den samme cloududbyders kunder eller samlede revisioner udført af en tredjepartsrevisor udpeget af en række kunder af samme cloududbyder.

38. Ved outsourcing af kritiske eller vigtige funktioner bør en virksomhed vurdere, om tredjepartscertificeringerne og de eksterne eller interne revisionsrapporter, der er anført

i punkt 37a, er egnede og fyldestgørende i henseende til at opfylde dens forpligtelser i henhold til gældende ret og bør tilstræbe ikke udelukkende at gøre brug af disse certificeringer og rapporter i længere tid.

39. Ved outsourcing af kritiske eller vigtige funktioner bør en virksomhed kun gøre brug af de tredjepartscertificeringer og eksterne eller interne revisionsrapporter, der er anført i punkt 37a, hvis den:

    a) finder, at certificeringerne eller revisionsrapporterne omfatter cloududbyderens centrale systemer (f.eks. processer, applikationer, infrastruktur, datacentre) de centrale kontroller, som selskabet har fastlagt, og overholdelse af relevant gældende ret
    b) løbende foretager en grundig vurdering af indholdet af certificeringerne eller revisionsrapporterne og verificerer, at certificeringerne eller rapporterne ikke er forældede
    c) sikrer, at cloududbyderens centrale systemer og kontroller indgår i fremtidige versioner af certificeringerne eller revisionsrapporterne
    d) accepterer den certificerende eller reviderende part (f.eks. på grundlag af disses kvalifikationer, ekspertise, genudførelse/-verificering af dokumentationen i den underliggende revisionsfil samt udskiftning af det certificerende eller reviderende selskab)
    e) finder, at certificeringerne er udstedt og revisionerne udført i henhold til anerkendte standarder, og at de indbefatter en test af effektiviteten af de centrale kontroller, der er etableret
    f) har en kontraktmæssig ret til at anmode om, at anvendelsesområdet for certificeringer eller revisionsrapporter udvides til andre af cloududbyderens relevante systemer og kontroller, idet antallet og hyppigheden af sådanne anmodninger om ændring af anvendelsesområdet bør have et rimeligt omfang, og idet anmodningerne bør være legitime ud fra et risikostyringsperspektiv
    g) bevarer den kontraktmæssige ret til at udføre individuelle revisioner på stedet efter eget skøn med hensyn til den outsourcede funktion.

40. En virksomhed bør sikre, at der inden et besøg på stedet, herunder også et besøg aflagt af en tredjepart, der er udpeget af virksomheden (f.eks. en revisor), gives forudgående meddelelse inden for rimelig tid til cloududbyderen, medmindre det ikke er muligt at give en sådan forudgående meddelelse på grund af en nødsituation eller en krisesituation, eller fordi det ville føre til en situation, hvor revisionen ikke længere ville være effektiv. I en sådan meddelelse bør være angivet stedet for og formålet med besøget og de medarbejdere, der deltager i besøget.

41. I betragtning af at cloudtjenester indebærer et højt niveau af teknisk kompleksitet og giver anledning til specifikke kompetencemæssige udfordringer, bør de medarbejdere, der udfører revisionen – uanset om der er tale om virksomhedens interne revisorer eller revisorer, der handler på egne vegne – have de relevante kompetencer og den relevante viden til at kunne foretage en korrekt vurdering af de pågældende cloudtjenester og udføre en effektiv og relevant revision. Dette bør også gælde de af

virksomhedens medarbejdere, der vurderer de certificeringer eller revisionsrapporter, der leveres af cloududbyderen.

Retningslinje 7. Videreoutsourcing

42. Hvis det er tilladt at videreoutsource kritiske eller vigtige funktioner (eller væsentlige dele deraf), bør den skriftlige cloudoutsourcingaftale mellem virksomheden og cloududbyderen:

    a) angive enhver del eller ethvert aspekt af den outsourcede funktion, der er undtaget fra potentiel videreoutsourcing
    b) angive de betingelser, der skal opfyldes i tilfælde af videreoutsourcing
    c) angive, at cloududbyderen fortsat er ansvarlig og er forpligtet til at føre tilsyn med de tjenester, cloududbyderen har videreoutsourcet, for at sikre, at alle kontraktmæssige forpligtelser mellem cloududbyderen og virksomheden til stadighed opfyldes
    d) omfatte en forpligtelse for cloududbyderen til at underrette virksomheden om enhver planlagt videreoutsourcing, eller væsentlige ændringer deraf, navnlig når dette kan påvirke cloududbyderens evne til at opfylde sine forpligtelser i medfør af outsourcingaftalen med virksomheden. Den underretningsperiode, der er fastsat i den skriftlige aftale, bør give virksomheden tilstrækkelig tid til som minimum at udføre en risikovurdering af den påtænkte videreoutsourcing, eller væsentlige ændringer deraf, og til at gøre indsigelse mod eller eksplicit godkende disse, som anført i punkt e) nedenfor
    e) sikre, at virksomheden har ret til at gøre indsigelse mod den påtænkte videreoutsourcing, eller væsentlige ændringer deraf, eller at eksplicit godkendelse er påkrævet, inden den påtænkte videreoutsourcing eller inden væsentlige ændringer træder i kraft
    f) sikre, at virksomheden har kontraktmæssig ret til at opsige cloudoutsourcingaftalen med cloududbyderen, hvis denne gør indsigelse mod den påtænkte outsourcing, eller væsentlige ændringer deraf, og i tilfælde af uretmæssig videreoutsourcing (f.eks. hvis cloududbyderen fortsætter videreoutsourcingen uden at underrette virksomheden, eller hvis cloududbyderen groft misligholder betingelserne for videreoutsourcing som anført i outsourcingaftalen).

43. Virksomheden bør sikre, at cloududbyderen fører det fornødne tilsyn med den, der videreoutsources til.

Retningslinje 8. Skriftlig underretning af kompetente myndigheder

44. Virksomheden bør i god tid skriftligt underrette sin kompetente myndighed om planlagte cloudoutsourcingaftaler, der vedrører en kritisk eller vigtig funktion. Virksomheden bør også i god tid skriftligt underrette sin kompetente myndighed om cloudoutsourcingaftaler, der vedrører en funktion, som tidligere var klassificeret som ikkekritisk eller ikkevigtig, men nu er blevet kritisk eller vigtig.

45. Virksomhedens skriftlige underretning bør under hensyntagen til proportionalitetsprincippet mindst omfatte følgende oplysninger:

    a) startdatoen for cloudoutsourcingaftalen og, hvis relevant, datoen for næste kontraktforlængelse, slutdatoen og/eller opsigelsesvarsler for cloududbyderen og for virksomheden
    b) en kort beskrivelse af den outsourcede funktion
    c) en kort redegørelse for årsagerne til, at den outsourcede funktion anses for kritisk eller vigtig
    d) cloududbyderens navn og handelsnavn (hvis et sådant findes), cloududbyderens registreringsland og registreringsnummer, cloududbyderens identifikator for juridisk enhed (hvis en sådan foreligger), cloududbyderens registrerede adresse og andre relevante kontaktoplysninger samt navnet på moderselskabet (hvis et sådant findes)
    e) lovvalg for cloudoutsourcingaftalen og, hvis et sådant findes, værneting
    f) cloudimplementeringsmodellerne og den specifikke karakter af de data, der outsources til cloududbyderen, og de steder (navnlig regioner eller lande), hvor disse data skal opbevares
    g) datoen for den seneste vurdering af, om den outsourcede funktion er kritisk eller vigtig
    h) datoen for den seneste risikovurdering eller revision af cloududbyderen sammen med en kort redegørelse for de væsentligste resultater, samt datoen for den næste planlagte risikovurdering eller revision
    i) den person eller det beslutningstagende organ i virksomheden, der har godkendt cloudoutsourcingaftalen
    j) hvis relevant, navnene på enhver, som væsentlige dele af en kritisk eller vigtig funktion er videreoutsourcet til, herunder det land eller region, hvor de, der videreoutsources til, er registreret, hvor den videreoutsourcede tjeneste vil blive udført, og hvor dataene skal opbevares.

Retningslinje 9. Tilsyn med cloudoutsourcingaftaler

46. De kompetente myndigheder bør som led i deres tilsynsproces foretage en vurdering af de risici, virksomheders cloudoutsourcingaftaler indebærer. Ved vurderingen bør myndighederne navnlig fokusere på aftaler, der vedrører outsourcing af kritiske eller vigtige funktioner.

47. De kompetente myndigheder bør kontrollere, at de kan udføre et effektivt tilsyn, navnlig når virksomheder outsourcer kritiske eller vigtige funktioner, der udføres uden for EU.

48. De kompetente myndigheder bør på grundlag af en risikobaseret tilgang vurdere, om virksomheder:

    a) har etableret relevante governance-processer samt ressource- og driftsmæssige processer til i fornødent omfang og reelt at indgå, implementere og føre tilsyn med cloudoutsourcingaftaler
    b) identificerer og styrer alle relevante risici, der er forbundet med cloudoutsourcingaftalen.

49. Hvis der identificeres koncentrationsrisici, bør de kompetente myndigheder overvåge udviklingen af sådanne risici og vurdere både disses potentielle konsekvenser for andre virksomheder, som de fører tilsyn med, og det finansielle markeds stabilitet.