EBA/REC/2017/03

28/03/2018

# Henstillinger

## om outsourcing til cloudserviceudbydere

# 1. Efterlevelses- og indberetningspligt

## Henstillingernes status

1. Dette dokument indeholder henstillinger udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010[1]. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve disse henstillinger bedst muligt.

2. Henstillinger afspejler EBA's syn på passende tilsynspraksis inden for det europæiske finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omhandlet i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af henstillingerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller deres tilsynsprocesser), også hvor henstillingerne primært er rettet mod institutioner.

## Indberetningspligt

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest 28.05.2018 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse henstillinger, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve henstillingerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, til compliance@eba.europa.eu med referencen "EBA/REC/2017/03". Underretninger fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

# 2. Emne, anvendelsesområde og definitioner

## Emne og anvendelsesområde

1. Henstillingerne indeholder en nærmere præcisering af de betingelser for outsourcing, der er beskrevet i Det Europæiske Banktilsynsudvalgs (CEBS) retningslinjer for outsourcing af 14. december 2006, og finder anvendelse på outsourcing, der foretages af de institutter, der er defineret i artikel 4, stk. 1, nr. 3), i forordning (EU) nr. 575/2013, til cloudserviceudbydere.

## Adressater

2. Disse henstillinger er rettet til de kompetente myndigheder, der er defineret i artikel 4, stk. 2, nr. i), i forordning (EU) nr. 1093/2010, og til de institutter, der er defineret i artikel 4, stk. 1, nr. 3), i forordning (EU) nr. 575/2013.[2]

## Definitioner

3. Medmindre andet er angivet, har de udtryk, der er anvendt og defineret i direktiv 2013/36/EU[3] om kapitalkrav og i CEBS' retningslinjer, den samme betydning i henstillingerne. I disse henstillinger finder endvidere følgende definitioner anvendelse:

| | |
|---|---|
| Cloudservice | Serviceydelse leveret ved hjælp af cloudcomputing, dvs. en model, der tillader lettilgængelig og -anvendelig on demand-netværksadgang til en fælles pulje af konfigurerbare computerressourcer (f.eks. netværk, servere, lagring, applikationer og serviceydelser), som hurtigt kan leveres og idriftsættes med et minimum af administration eller interaktion med serviceudbyderen. |
| Offentlig cloud | Cloudinfrastruktur, som kan anvendes af offentligheden. |
| Privat cloud | Cloudinfrastruktur, som udelukkende kan anvendes af ét institut. |
| Fælles cloud | Cloudinfrastruktur, som kan anvendes af en bestemt gruppe institutter, herunder flere institutter i en koncern. |

[2] Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012.

[3] Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF.

| | |
|---|---|
| Hybrid cloud | Cloudinfrastruktur, som består af to eller flere særskilte cloudinfrastrukturer. |

# 3. Gennemførelse

## Anvendelsesdato

5. Disse henstillinger finder anvendelse fra den 1. juli 2018.

# 4. Henstillinger om outsourcing til cloudserviceudbydere

## 4.1 Vurdering af væsentlighed

1. De outsourcende institutter bør forud for outsourcingen af deres aktiviteter vurdere, hvilke aktiviteter der anses for væsentlige. Institutterne bør udføre denne vurdering af aktiviteternes væsentlighed på grundlag af retningslinje 1, litra f), i CEBS' retningslinjer og for så vidt angår outsourcing til cloudserviceudbydere bør der i særdeleshed tages hensyn til følgende:

    (a) den kritiske karakter af og den iboende risikoprofil for de aktiviteter, der skal outsources, dvs. om der tale om aktiviteter, der er kritiske for instituttets forretningskontinuitet/levedygtighed og dets forpligtelser over for kunderne

    (b) de direkte driftsmæssige konsekvenser af afbrydelser og beslægtede retslige og omdømmerelaterede risici

    (c) de konsekvenser, som en eventuel afbrydelse af aktiviteten ville kunne få for instituttets indtægter

    (d) de mulige konsekvenser, som et brud på fortroligheden eller dataintegriteten kan få for instituttet og dets kunder.

## 4.2 Pligt til at informere de tilsynsførende tilstrækkeligt

2. De outsourcende institutter bør i tilstrækkeligt omfang informere de kompetente myndigheder om væsentlige aktiviteter, der skal outsources til cloudserviceudbydere. Institutterne bør gøre dette på grundlag af afsnit 4.3 i CEBS og i alle tilfælde stille følgende oplysninger til rådighed for de kompetente myndigheder:

    (a) navnet på cloudserviceudbyderen og navnet på moderselskabet (hvis relevant)
    (b) en beskrivelse af de aktiviteter og data, der skal outsources
    (c) det land eller de lande, hvor serviceydelsen skal udføres (herunder datalokaliseringen)
    (d) serviceydelsens startdato
    (e) den seneste kontraktfornyelsesdato (hvis relevant)
    (f) den gældende lovgivning for kontrakten
    (g) serviceydelsens udløbsdato eller næste kontraktfornyelsesdato (hvis relevant).

3. Ud over de oplysninger, der fremlægges i overensstemmelse med forrige afsnit, kan den kompetente myndighed anmode det outsourcende institut om yderligere oplysninger om dets risikoanalyse med hensyn til de væsentlige aktiviteter, der skal outsources, såsom:

(a) hvorvidt cloudserviceudbyderen har en beredskabsplan, der er hensigtsmæssig for de serviceydelser, der ydes for det outsourcende institut
(b) hvorvidt det outsourcende institut har en exitstrategi i tilfælde af, at en af parterne bringer kontrakten til ophør eller cloudserviceudbyderen ophører med at levere servicerne
(c) hvorvidt det outsourcende institut opretholder de fornødne færdigheder og ressourcer til behørigt at overvåge de outsourcede aktiviteter.

4. Det outsourcende institut bør føre et ajourført register med oplysninger om alle de væsentlige og ikke-væsentlige aktiviteter, der outsources til cloudserviceudbydere på institut- og koncernniveau. Det outsourcende institut bør til den kompetente myndighed efter anmodning stille en kopi af outsourcingaftalen og de beslægtede oplysninger, der er opført i registret, til rådighed, uanset om instituttet har vurderet den aktivitet, der blev outsourcet til en cloudserviceudbyder, som værende væsentlig eller ej.

5. Registeret, der henvises til i forrige afsnit, bør mindst indeholde følgende oplysninger:

(a) de oplysninger, der henvises til i afsnit 2, litra a)-g), hvis de ikke er fremlagt endnu
(b) outsourcingtype (cloudservicemodellen og cloudimplementeringsmodellen, dvs. offentlig/privat/hybrid/fælles cloud)
(c) de parter, der modtager cloudserviceydelsen som led i outsourcingaftalen
(d) dokumentation for ledelsens eller dets delegerede udvalgs godkendelse af outsourcingen, hvis relevant
(e) navn på eventuelle underleverandører, hvis relevant
(f) det land, hvor cloudserviceudbyderen/de vigtigste underleverandører er registreret
(g) hvorvidt outsourcingen er vurderet som værende væsentlig (ja/nej)
(h) dato for instituttets sidste væsentlighedsvurdering af de outsourcede aktiviteter
(i) hvorvidt cloudserviceudbyderen/underleverandøren(-erne) varetager forretningsaktiviteter, der er tidskritiske (ja/nej)
(j) en vurdering af, hvor let cloudserviceudbyderen kan erstattes (let, vanskeligt eller umuligt)
(k) identifikation af alternativserviceudbyder, om muligt
(l) dato for seneste risikovurdering af outsourcingen- eller videreoutsourcingen.

## 4.3 Ret til adgang og revision

### For institutter

6. På baggrund af retningslinje 8, stk. 2, litra g), i CEBS' retningslinjer og med henblik på cloudoutsourcing bør de outsourcende institutter endvidere sikre, at de har en skriftlig aftale med cloudserviceudbyderen, hvormed denne forpligter sig til at:

(a) sørge for fuld adgang til sine forretningslokaler (hovedkvarter og driftscentre), herunder samtlige enheder, systemer, netværk og data, der anvendes til at yde de outsourcede

serviceydelser (ret til adgang), for instituttet, en eventuel tredjepart, som instituttet udpeger hertil, og instituttets revisor

(b) tildele ubegrænset ret til inspektion og revision med relation til de outsourcede serviceydelser (ret til revision) for instituttet, en eventuel tredjepart, som instituttet udpeger hertil, og instituttets revisor.

7. Den faktiske udøvelse af adgangs- og revisionsretten bør ikke hindres eller begrænses af kontraktlige bestemmelser. Hvis udførelsen af revisionerne eller anvendelsen af visse revisionsteknikker kan udgøre en risiko for en anden kundes miljø, bør der aftales alternative måder at yde et lignende sikkerhedsniveau på, som påkrævet af instituttet.

8. Det outsourcende institut bør udøve sin ret til adgangs og revision med en risikobaseret tilgang. Hvis et outsourcende institut ikke har egne revisionsressourcer ansat hos sig, bør det overveje at gøre brug af et af følgende værktøjer:

(a) revisioner i puljer, der tilrettelægges i fællesskab med andre kunder hos den samme cloudserviceudbyder, og som udføres af disse kunder eller en tredjepart, der er udpeget af dem, for at anvende revisionsressourcerne mere effektivt og mindske den organisatoriske byrde både på kunderne og cloudserviceudbyderen.

(b) tredjepartscertificeringer og tredjeparts- eller interne revisionsrapporter, der stilles til rådighed af cloudserviceudbyderen, forudsat at:

i. det outsourcende institut sikrer, at anvendelsesområdet for certificeringen eller revisionsrapporten omfatter de systemer (dvs. processer, applikationer, infrastruktur, datacentre mv.) og kontroller, som det outsourcende institut har udpeget som centrale
ii. det outsourcende institut foretager løbende en grundig vurdering af certificeringernes eller revisionsrapporternes indhold og sikrer navnlig, at de centrale kontroller stadig er indbefattet i senere udgaver af en revisionsrapport, samt kontrollerer, at certificeringen eller revisionsrapporten ikke er forældet
iii. det outsourcende institut er tilfreds med certificerings- eller revisionspartens formåen (f.eks. med hensyn til rotation i certificerings- eller revisionsfirmaet, kvalifikationer, ekspertise, genudførelse/kontrol af revisionsbeviset i de underliggende stamoplysninger)
iv. certificeringerne og revisionerne udføres i henhold til anerkendte standarder og indbefatter en test af de vigtigste eksisterende kontrollers operationelle effektivitet
v. det outsourcende institut har kontraktlig ret til at anmode om, at certificeringernes eller revisionsrapporternes anvendelsesområde udvides til bestemte systemer og/eller kontroller, der er relevante. Antallet og hyppigheden af disse anmodninger om ændring af anvendelsesområdet bør være rimelige – og berettigede ud fra et risikostyringsperspektiv.

9. I betragtning af, at cloudløsninger har et højt teknisk kompleksitetsniveau, bør det outsourcende institut efterprøve, om de medarbejdere, der udfører revisionen – hvad enten det er interne revisorer eller den pulje af revisorer, der handler på deres vegne, eller de revisorer, som cloudserviceudbyderen har udpeget – eller om de medarbejdere, alt efter tilfældet, der gennemgår tredjepartscertificeringen eller serviceudbyderens revisionsrapport, besidder de rette færdigheder og den rette viden til at kunne udføre effektive og relevante revisioner og/eller vurderinger af cloudløsninger.

### For kompetente myndigheder

10. I henhold til retningslinje 8, stk. 2, litra h), i CEBS' retningslinjer og med henblik på cloudoutsourcing bør outsourcende institutter sikre, at de har en skriftlig aftale med cloudserviceudbyderen, hvormed denne forpligter sig til:

    (a) at sørge for fuld adgang til cloudserviceudbyderens forretningslokaler (hovedkvarter og driftscentre), herunder samtlige enheder, systemer, netværk og data, der anvendes til at yde serviceydelser til det outsourcende institut (adgangsret), for den kompetente myndighed, der fører tilsyn med det outsourcende institut (eller en eventuel tredjepart, som myndigheden udpeger hertil)

    (b) at tildele ubegrænset ret til inspektion og revision i relation til de outsourcede serviceydelser (ret til revision) for den kompetente myndighed, der fører tilsyn med det outsourcende institut (eller en eventuel tredjepart, som myndigheden udpeger hertil).

11. Det outsourcende institut bør sikre, at de kontraktlige bestemmelser ikke hindrer den kompetente myndighed i at udføre sin tilsynsfunktion og sine tilsynsmålsætninger.

12. Oplysninger, som de kompetente myndigheder får i forbindelse med adgangs- og revisionsretten, bør være underlagt den tavshedspligt og de fortrolighedskrav, der henvises til i artikel 53 ff. i direktiv 2013/36/EU (CRD IV). De kompetente myndigheder bør afstå fra at indgå i enhver form for kontraktlig aftale eller erklæring, der forhindrer dem i at overholde EU-rettens bestemmelser om fortrolighed, tavshedspligt og informationsudveksling.

13. De kompetente myndigheder bør på baggrund af revisionsresultaterne påpege eventuelle identificerede mangler, om nødvendigt, ved at indføre foranstaltninger direkte på det outsourcende institut.

## 4.4 Hvad særligt angår retten til adgang

14. Aftalen, der er nævnt i stk. 6 og 10, bør bl.a. omfatte følgende bestemmelser:

    (a) Den part, der har til hensigt at udøve sin adgangsret (institut, kompetent myndighed, revisor eller tredjepart, der handler på vegne af instituttet eller den kompetente myndighed), bør inden for en rimelig tidsfrist forud for et

planlagt besøg varsle det pågældende forretningssted herom, medmindre et forudgående varsel ikke har været muligt grundet en nød- eller krisesituation.

(b) Det påkræves, at cloudserviceudbyderen samarbejder fuldt ud med de behørige kompetente myndigheder samt med instituttet og dets revisor i forbindelse med besøget på stedet.

## 4.5 Data- og systemsikkerhed

15. Som angivet i retningslinje 8, stk. 2, litra e), i CEBS' retningslinjer, bør outsourcingkontrakten forpligte outsourcingudbyderen til at beskytte fortroligheden af de oplysninger, som sendes af det finansielle institut. I overensstemmelse med retningslinje 6, stk. 6, litra e), i CEBS' retningslinjer bør institutterne implementere bestemmelser for at sikre tilgængeligheden af de serviceydelser, der leveres af outsourcingudbydere. På baggrund af retningslinje 8, stk. 2, litra b), og retningslinje 9 i CEBS' retningslinjer bør de outsourcende institutters respektive behov med hensyn til kvalitet og udførelse indgå i skriftlige outsourcingkontrakter og serviceaftaler. Disse sikkerhedsaspekter bør desuden overvåges løbende (retningslinje 7).

16. Med henblik på formålene i forrige afsnit bør instituttet forud for outsourcingen og med henblik på at understøtte den pågældende beslutning som minimum udføre følgende:

(a) identificere og klassificere sine aktiviteter, processer og beslægtede data og systemer ud fra følsomhed og påkrævet beskyttelse

(b) udføre en grundig risikobaseret udvælgelse af de aktiviteter, processer og relaterede data og systemer, som det overvejes at outsource til en cloudløsning

(c) definere og fastlægge et passende beskyttelsesniveau for datafortroligheden, kontinuiteten af de outsourcede aktiviteter og integriteten og sporbarheden af dataene og systemerne i forbindelse med den tilsigtede cloudoutsourcing. Institutterne bør endvidere overveje specifikke foranstaltninger, hvor det er relevant, for data i overførsel, data i behandling og data i lagring, som f.eks. anvendelse af krypteringsteknologier i kombination med passende styring af krypteringsnøgler.

17. Institutter bør sikre, at de har en skriftlig aftale med cloudserviceudbyderen, hvor forpligtelser mv. i henhold til afsnit 16, litra c), fastsættes.

18. Institutter bør løbende overvåge aktiviteterne og sikkerhedsforanstaltningerne i overensstemmelse med retningslinje 7 i CEBS' retningslinjer, herunder hændelser, og løbende gennemgå, om outsourcingen af deres aktiviteter er i overensstemmelse med de forrige afsnit. De bør straks foretage eventuelle påkrævede udbedrende foranstaltninger.

## 4.6 Data- og databehandlingsbeliggenhed

19. Som angivet i retningslinje 4, stk. 4, i CEBS' retningslinjer, bør institutterne være særlig opmærksomme, når de indgår og administrerer outsourcingaftaler uden for EØS, på grund af mulige databeskyttelsesrisici og risici vedrørende effektivt tilsyn foretaget af tilsynsmyndigheden.

20. Det outsourcende institut bør have en risikobaseret tilgang til overvejelser om data- og databehandlingsbeliggenheden, når der outsources til et cloudmiljø. Vurderingen bør tage hensyn til de potentielle konsekvenser af risiciene, herunder retlige risici og complianceproblemer og begrænsninger i overvågningen i de lande, hvor de outsourcede serviceydelser skal eller sandsynligvis skal ydes, og hvor dataene skal eller sandsynligvis skal lagres. Vurderingen bør omfatte overvejelser om den bredere politiske og sikkerhedsmæssige stabilitet i de pågældende jurisdiktioner, om de gældende love i disse jurisdiktioner (herunder love om databeskyttelse) og om de foreliggende retshåndhævelsesbestemmelser i disse jurisdiktioner, herunder de lovbestemmelser om insolvens, der vil gælde, hvis en cloudserviceudbyder går fallit. Det outsourcende institut bør sikre, at disse risici holdes inden for acceptable niveauer, der står i et rimeligt forhold til den outsourcede aktivitet.

## 4.7 Videreoutsourcing

21. Som angivet i retningslinje 10 i CEBS' retningslinjer, bør institutterne tage hensyn til risici forbundet med videreoutsourcing, hvor outsourcingudbyderen videreoutsourcer dele af serviceydelsen til andre udbydere. Det outsourcende institut bør kun indvilge i videreoutsourcing, hvis underleverandøren også fuldt ud vil overholde de eksisterende forpligtelser mellem det outsourcende institut og outsourcingudbyderen. Derudover bør det outsourcende institut træffe passende foranstaltninger til at tage hensyn til risikoen for enhver svaghed eller mangel i ydelsen af de aktiviteter, der er videreoutsourcet og som har en betydelig indvirkning på outsourcingudbyderens evne til at opfylde sine forpligtelser i henhold til outsourcingaftalen.

22. Outsourcingaftalen mellem det outsourcende institut og cloudserviceudbyderen bør angive alle typer aktiviteter, der er udelukket fra mulig videreoutsourcing, og anføre, at cloudserviceudbyderen har det fulde ansvar for og skal have overblik over serviceydelser, som er videreoutsourcet.

23. Outsourcingaftalen bør endvidere omfatte en forpligtelse for cloudserviceudbyderen til at oplyse det outsourcende institut om alle planlagte betydelige ændringer hos underleverandørerne eller af underleverandørens serviceydelser, som er opstillet i den oprindelige aftale, og som ville kunne påvirke serviceudbyderens evne til at opfylde sine forpligtelser i outsourcingaftalen. Notifikationsperioden for disse ændringer bør være fastlagt på forhånd i en kontrakt for at gøre det muligt for det outsourcende institut at udføre en risikovurdering af konsekvenserne af de foreslåede ændringer, inden de faktiske ændringer gennemføres hos underleverandørerne eller af underleverandørernes serviceydelser.

24. I tilfælde af, at en cloudserviceudbyder planlægger ændringer hos en underleverandør eller de videreoutsourcede serviceydelser, der vil have en negativ indvirkning på risikovurderingen af de aftalte serviceydelser, bør det outsourcende institut have ret til at bringe kontrakten til ophør.

25. Det outsourcende institut bør løbende vurdere med og overvåge kvaliteten af den samlede serviceydelse, uanset om den ydes af cloudserviceudbyderen eller dennes underleverandører.

## 4.8 Beredskabsplaner og exitstrategier

26. Som angivet i retningslinje 6, stk. 1, retningslinje 6, stk. 6, litra e), og retningslinje 8, stk. 2, litra d), i CEBS' retningslinjer, bør det outsourcende institut planlægge og gennemføre foranstaltninger til at opretholde kontinuiteten af dets forretning, såfremt en outsourcingudbyder går fallit eller kvaliteten af dennes arbejde falder til et uacceptabelt niveau. Disse bestemmelser bør omfatte beredskabsplanlægning og en tydeligt formuleret exitstrategi. Desuden bør outsourcingkontrakten omfatte en opsigelses- og exitklausul, der muliggør, at aktiviteterne, der er leveret af outsourcingudbyderen, kan overføres til en anden outsourcingudbyder, eller kan hjemtages til det outsourcende institut.

27. Et outsourcende institut bør desuden sikre, at det er i stand til at trække sig ud af aftalen om cloudoutsourcing, hvis det er relevant, uden at det unødigt afbryder leveringen af serviceydelser, får en negativ virkning på instituttets overholdelse af de regulatoriske bestemmelser eller forringer kontinuiteten og kvaliteten af dets levering af serviceydelser til kunderne. For at gennemføre dette bør det outsourcende institut:

    (a) udvikle og gennemføre exitplaner, der er omfattende, dokumenterede og tilstrækkeligt afprøvede, hvis relevant

    (b) identificere alternative løsninger og udvikle overgangsplaner, så det er muligt at fjerne og overføre eksisterende aktiviteter og data fra cloudserviceudbyderen til disse løsninger på en kontrolleret og tilstrækkeligt afprøvet måde, hvor der tages hensyn til problemer vedrørende databeliggenhed og opretholdelse af forretningskontinuitet tilgængelighed i løbet af overgangsfasen

    (c) sikre, at outsourcingaftalen forpligter cloudserviceudbyderen til at hjælpe det outsourcende institut tilstrækkeligt med at overføre aktiviteten til en anden udbyder eller til det outsourcende institut i tilfælde af ophævelse af outsourcingaftalen.

28. Under udarbejdelsen af exitstrategierne bør det outsourcende institut overveje følgende:

    (a) udvikle centrale risikoindikatorer til at identificere et uacceptabelt serviceniveau

    (b) udføre en konsekvensanalyse, der står i rimeligt forhold til de outsourcede aktiviteter, for at fastlægge, hvilke menneskelige og materielle ressourcer der vil være påkrævet for at gennemføre exitplanen, og hvor lang tid det vil tage

(c) tildele roller og ansvarsområder med henblik på styringen af exitplanerne og overgangene

(d) fastlægge succeskriterier for overgangen.

29. Det outsourcende institut bør anføre indikatorer, der kan udløse exitplanen under den løbende overvågning af og tilsyn med de serviceydelser, der leveres af cloudserviceudbyderen.