

EBA/GL/2019/02

---

25. februar 2019

---

# Retningslinjer for outsourcing

---

# 1. Compliance- og indberetningsforpligtelser

---

## Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010.<sup>1</sup> I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 bestræber de kompetente myndigheder og finansielle institutioner sig bedst muligt på at efterleve disse retningslinjer.
2. Retningslinjerne 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 defineret i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, som er omfattet af retningslinjerne, 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 retningslinjerne primært er rettet mod institutter og betalingsinstitutter.

## Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den [dd.mm.yyyy] underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Meddeles dette ikke EBA inden for den angivne frist, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Meddelelser bør indsendes på formularen, der er tilgængelig på EBA's websted, til [compliance@eba.europa.eu](mailto:compliance@eba.europa.eu) med referencen "EBA/GL/2019/02". Meddelelser bør indsendes af personer med bemyndigelse til at indgive meddelelse om efterlevelse på vegne af de pågældende kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også meddeles EBA.
4. Meddelelser offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

---

<sup>1</sup> 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. Formål, anvendelsesområde og definitioner

---

### Emne

5. I disse retningslinjer fastsættes de interne ledelsesordninger, herunder forsvarlig risikostyring, som institutter, betalingsinstitutter og udstedere af elektroniske penge bør gennemføre, når de outsourcer funktioner, navnlig i forbindelse med outsourcing af kritiske eller vigtige funktioner.
6. Retningslinjerne præciserer, hvordan de ordninger, der er omhandlet i foregående afsnit, bør vurderes og overvåges af de kompetente myndigheder i overensstemmelse med artikel 97 i direktiv 2013/36/EU<sup>2</sup>, tilsyns kontrol- og vurderingsprocessen (SREP), artikel 9, stk. 3, i direktiv (EU) 2015/2366<sup>3</sup> og artikel 5, stk. 5, i direktiv 2009/110/EF<sup>4</sup>, ved at de udfører deres pligt til at overvåge, at enheder, som disse retningslinjer er rettet mod, løbende opfylder betingelserne for tilladelse.

### Målgrupper

7. Målgruppen for disse retningslinjer er kompetente myndigheder som defineret i artikel 4, stk. 1, nr. 40, i forordning (EU) nr. 575/2013<sup>5</sup>, herunder Den Europæiske Centralbank med hensyn til forhold, der vedrører de opgaver, den er pålagt ved forordning (EU) nr. 1024/2013<sup>6</sup>, institutter som defineret i artikel 4, stk. 1, nr. 3, i forordning (EU) nr. 575/2013, betalingsinstitutter som defineret i artikel 4, stk. 4, i direktiv 2015/2366/EU, og udstedere af elektroniske penge, jf. artikel 2, stk. 1, i direktiv 2009/110/EF. Kontooplysningstjenesteudbydere, der kun leverer tjenesten i punkt 8 i bilag I til direktiv (EU) 2015/2366, er ikke omfattet af disse retningslinjers anvendelsesområde i overensstemmelse med artikel 33 i nævnte direktiv.

---

<sup>2</sup> 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.

<sup>3</sup> Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF.

<sup>4</sup> Europa-Parlamentets og Rådets direktiv 2009/110/EF af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF

<sup>5</sup> 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 (EUT L 176 af 27.6.2013, s. 1).

<sup>6</sup> Rådets forordning (EU) nr. 1024/2013 af 15. oktober 2013 om overdragelse af specifikke opgaver til Den Europæiske Centralbank i forbindelse med politikker vedrørende tilsyn med kreditinstitutter.

8. I disse retningslinjer forstås ved "betalingsinstitutter" også "e-pengeinstitutter", og enhver henvisning til "betalingstjenester" omfatter "udstedelse af elektroniske penge".

## Anvendelsesområde

9. Med forbehold for direktiv 2014/65/EU<sup>7</sup> og Kommissionens delegeret forordning (EU) nr. 2017/565<sup>8</sup> (som indeholder krav vedrørende outsourcing fra institutter, der yder investeringsservice og udfører investeringsaktiviteter, samt relevante retningslinjer udstedt af Den Europæiske Værdipapir- og Markedstilsynsmyndighed vedrørende investeringsservice og -aktiviteter), bør institutter som defineret i artikel 3, stk. 1, nr. 3, i direktiv 2013/36/EU overholde disse retningslinjer på et individuelt, delkonsolideret og konsolideret niveau. De kompetente myndigheder kan undtage, at retningslinjerne finder anvendelse på individuelt niveau, jf. artikel 21 i direktiv 2013/36/EU eller artikel 109, stk. 1, i direktiv 2013/36/EU, sammenholdt med artikel 7 i forordning (EU) nr. 575/2013. Institutter, der er omfattet af direktiv 2013/36/EU, bør overholde dette direktiv og disse retningslinjer på konsolideret og delkonsolideret niveau, jf. artikel 21 og artikel 108-110 i direktiv 2013/36/EU.
10. Betalingsinstitutter og udstedere af elektroniske penge bør overholde disse retningslinjer på individuelt niveau, jf. dog artikel 8, stk. 3, i direktiv (EU) 2015/2366 og artikel 5, stk. 7, i direktiv 2009/110/EF.
11. De kompetente myndigheder med ansvar for tilsyn med institutter, betalingsinstitutter og udstedere af elektroniske penge bør overholde disse retningslinjer.

## Definitioner

12. Medmindre andet er angivet, har de termer, der er anvendt og defineret i direktiv 2013/36/EU, forordning (EU) nr. 575/2013, direktiv 2009/110/EF, direktiv (EU) 2015/2366 og EBA-retningslinjerne vedrørende intern ledelse<sup>9</sup> samme betydning i disse retningslinjer. I disse retningslinjer gælder derudover følgende definitioner:

Outsourcing

enhver form for ordning mellem et institut, et betalingsinstitut eller et e-pengeinstitut og en leverandør, i henhold til hvilken leverandøren udfører en proces, en tjenesteydelse eller en aktivitet, som instituttet, betalingsinstituttet eller udstederen af elektroniske penge ellers selv ville udføre.

---

<sup>7</sup> 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 (EUT L 173 af 12.6.2014, s. 349).

<sup>8</sup> 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 (EUT L 87 af 31.3.2017, s. 1-83).

<sup>9</sup> <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->

Funktion	alle processer, tjenesteydelser eller aktiviteter.
Kritisk eller vigtig funktion <sup>10</sup>	enhver funktion, der anses for kritisk eller vigtig som beskrevet i afsnit 4 i disse retningslinjer.
Videreoutsourcing	en situation, hvor en leverandør under en outsourcingordning videreoverdrager en yderligere outsourcet funktion til en anden underleverandør. <sup>11</sup>
Leverandør	en tredjepartsenhed, der udfører en outsourcet proces, tjenesteydelse eller aktivitet eller dele deraf i henhold til en outsourcingordning.
Cloudservice	tjenesteydelser leveret ved hjælp af cloudcomputing, dvs. en model, der tillader lettilgængelig og letanvendelig on demand-netværksadgang til en fælles pulje af konfigurerbare computerressourcer (f.eks. netværk, servere, lagring, applikationer og tjenesteydelser), som hurtigt kan leveres og idriftsættes med et minimum af administration eller interaktion med leverandøren.
Offentlig cloud	cloudinfrastruktur, som kan anvendes af offentligheden.
Privat cloud	cloudinfrastruktur, som udelukkende kan anvendes af ét institut eller betalingsinstitut.
Fælles cloud	cloudinfrastruktur, som kan anvendes af en bestemt gruppe institutter eller betalingsinstitutter, herunder flere institutter i én koncern.
Hybrid cloud	cloudinfrastruktur, som består af to eller flere særskilte cloudinfrastrukturer.
Ledelsesorgan	et instituts eller betalingsinstituttets organ eller ledelsesorganer, som er udpeget i overensstemmelse med national lovgivning, og som har beføjelse til at fastlægge instituttets eller betalingsinstituttets strategi, mål og generelle retning, og som fører tilsyn med og overvåger ledelsens beslutninger og omfatter de personer, der reelt leder instituttets eller betalingsinstituttets virksomhed, og de ansvarlige for ledelsen af betalingsinstituttet.

<sup>10</sup> Udtrykket "kritisk eller vigtig funktion" er baseret på den ordlyd, der anvendes i henhold til direktiv 2014/65/EU (MiFID II) og Kommissionens delegerede forordning (EU) 2017/565 om supplerende regler til MiFID II og anvendes kun med henblik på outsourcing; det vedrører ikke definitionen af "kritiske funktioner" i forbindelse med regelsættet for genopretning og afvikling som defineret i artikel 2, stk. 1, nr. (35) i direktiv 2014/59/EU.

<sup>11</sup> Bestemmelserne i afsnit 3 finder anvendelse på vurderingen; videreoutsourcing er også nævnt i andre EBA-dokumenter som en "kæde af outsourcing" eller "kædeoutsourcing".

## 3. Gennemførelse

---

### Anvendelsesdato

13. Med undtagelse af stk. 63, litra b, finder disse retningslinjer fra den 30. september 2019 anvendelse på alle outsourcingordninger, der indgås, revurderes eller ændres på eller efter denne dato. Stk. 63, litra b, finder anvendelse fra den 31. december 2021.
14. Institutter og betalingsinstitutter bør revurdere og ændre eksisterende outsourcingordninger med henblik på at sikre, at disse er i overensstemmelse med disse retningslinjer.
15. Hvis revurderingen af outsourcingordninger af kritiske eller vigtige funktioner ikke er afsluttet senest den 31. december 2021, bør institutter og betalingsinstitutter underrette deres kompetente myndighed herom, herunder om de foranstaltninger, der er planlagt for at afslutte revurderingen eller den mulige exitstrategi.

### Overgangsbestemmelser

16. Institutterne og betalingsinstitutterne bør supplere dokumentationen af alle eksisterende outsourcingordninger med undtagelse af outsourcingordninger til udbydere af cloudtjenester i overensstemmelse med disse retningslinjer efter den første udløbsdato for hver eksisterende outsourcingordning, dog senest den 31. december 2021.

### Ophævelse

17. Retningslinjerne fra Det Europæiske Banktilsynsudvalg (CEBS) om outsourcing af 14. december 2006 og EBA's henstillinger om outsourcing til udbydere af cloudtjenester<sup>12</sup> ophæves med virkning fra den 30. september 2019.

---

<sup>12</sup> Henstillinger om outsourcing til cloudserviceudbydere (EBA/REC/2017/03).

## 4. Retningslinjer for outsourcing

---

### Del I – Proportionalitet: koncerner og institutsikringsordninger

#### 1 Proportionalitet

18. Institutter, betalingsinstitutter og kompetente myndigheder bør, når de opfylder eller fører tilsyn med overholdelsen af disse retningslinjer, tage hensyn til proportionalitetsprincippet. Proportionalitetsprincippet har til formål at sikre, at forvaltningsordninger, herunder dem, der vedrører outsourcing, stemmer overens med instituttets eller betalingsinstituttets individuelle risikoprofil, art og forretningsmodel samt omfanget og kompleksiteten af deres aktiviteter, således at målene for myndighedskravene rent faktisk opnås.
19. Ved anvendelsen af de krav, der er fastsat i disse retningslinjer, skal institutter og betalingsinstitutter tage hensyn til kompleksiteten af de outsourcete funktioner, de risici, som følger af outsourcingordningen, hvor kritisk eller vigtig den outsourcete funktion er, og de potentielle konsekvenser af outsourcingen for kontinuiteten af deres aktiviteter.
20. Ved anvendelse af proportionalitetsprincippet skal institutter, betalingsinstitutter<sup>13</sup> og kompetente myndigheder tage hensyn til de kriterier, der er anført i del I i EBA's retningslinjer for intern ledelse i overensstemmelse med artikel 74, stk. 2, i direktiv 2013/36/EU.

#### 2 Outsourcing i koncerner og institutter, der er medlem af en institutsikringsordning

21. I henhold til artikel 109, stk. 2, i direktiv 2013/36/EU bør disse retningslinjer også gælde på et delkonsolideret og konsolideret grundlag under hensyntagen til den tilsynsmæssige konsolidering<sup>14</sup>. Til dette formål bør EU-moderselskaber eller moderselskabet i en medlemsstat sikre, at interne ledelsesordninger, processer og mekanismer i deres datterselskaber, herunder betalingsinstitutter, er konsistente, velintegrerede og passende for en effektiv anvendelse af disse retningslinjer på alle relevante niveauer.

---

<sup>13</sup> Betalingsinstitutter bør også henvise til EBA's retningslinjer i henhold til det andet betalingstjenestedirektiv om de oplysninger, der skal gives med hensyn til godkendelse af betalingsinstitutter og elektroniske pengeinstitutter samt registrering af kontooplysningstjenesteudbydere, som er tilgængelige på EBA's websted under følgende link: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2>

<sup>14</sup> Se artikel 4, stk. 1, nr. 47) og 48), i forordning (EU) nr. 575/2013 om omfanget af konsolideringen.

22. Institutter og betalingsinstitutter i overensstemmelse med punkt 21 og institutter, der som medlemmer af en institutsikringsordning bruger centralt bestemte ledelsesordninger, skal opfylde følgende:
- a. Hvor disse institutter eller betalingsinstitutter har outsourcingordninger med tjenesteudbydere inden for koncernen eller institutsikringsordningen <sup>15</sup>, har ledelsesorganet for disse institutter eller betalingsinstitutter også for disse outsourcingordninger det fulde ansvar for at overholde alle myndighedskrav og effektiv anvendelse af disse retningslinjer.
  - b. Hvor disse institutter eller betalingsinstitutter outsourcer de operationelle opgaver, der skal varetages inden for de interne kontrolfunktioner, til en tjenesteudbyder inden for koncernen eller institutsikringsordningen med henblik på overvågning og revision af outsourcingordninger, bør institutterne sikre, at disse outsourcingordninger udføres effektivt, herunder gennem modtagelse af passende rapporter.
23. Ud over punkt 22 bør institutter og betalingsinstitutter i en gruppe, som der ikke er givet nogen dispensationer i henhold til artikel 109 i direktiv 2013/36/EU og artikel 7 i forordning (EU) nr. 575/2013, og institutter, der er et centralt organ, eller som er varigt tilknyttet et centralt organ, som der ikke er givet nogen dispensationer i henhold til artikel 21 i direktiv 2013/36/EU, eller institutter, der er medlem af en institutsikringsordning, tage hensyn til følgende:
- a. Hvor den operationelle overvågning af outsourcing er centraliseret (f.eks. som en del af en rammeaftale for overvågning af outsourcingordninger), bør institutter og betalingsinstitutter sikre, at der i det mindste for outsourcete kritiske eller vigtige funktioner både er mulighed for uafhængig overvågning af tjenesteudbyderen og hensigtsmæssigt tilsyn med det enkelte institut eller betalingsinstitut, herunder ved mindst en gang årligt og efter anmodning fra den centraliserede overvågningsfunktion at modtage rapporter, der indeholder mindst et sammendrag af risikovurderingen og en resultatovervågning. Desuden bør institutter og betalingsinstitutter fra den centraliserede overvågningsfunktion modtage et sammendrag af de relevante revisionsrapporter med henblik på kritisk eller vigtig outsourcing og, efter anmodning, den fulde revisionsrapport.
  - b. Institutter og betalingsinstitutter bør sikre, at deres ledelsesorgan underrettes behørigt om relevante planlagte ændringer vedrørende tjenesteudbydere, der overvåges centralt, og de potentielle konsekvenser af disse ændringer for de kritiske eller vigtige funktioner, herunder et sammendrag af risikoanalysen med juridiske risici, overholdelse af lovregulerede krav og indvirkningen på serviceniveauet, så de kan vurdere konsekvenserne af disse ændringer.

---

<sup>15</sup> I overensstemmelse med artikel 113, stk. 7, i kapitalkravsforordningen er en institutsikringsordning en kontraktmæssig eller vedtægtsmæssig ansvarsordning, der beskytter disse institutter, som er medlemmer af ordningen, og navnlig sikrer deres likviditet og solvens for at undgå konkurs, når det er nødvendigt.



- c. Hvor disse institutter og betalingsinstitutter i koncernen, institutter tilknyttet et centralt organ eller institutter, som er en del af en institutsikringsordning, benytter en central forhåndsvurdering af outsourcingordninger som nævnt i artikel 12, bør det enkelte institut og betalingsinstitut modtage et sammendrag af vurderingen og sikre, at der tages hensyn til dets særlige struktur og risici i beslutningsprocessen.
  - d. Hvor registret over alle eksisterende outsourcingordninger som nævnt i artikel 11 etableres og vedligeholdes centralt i en koncern eller institutsikringsordning, bør de kompetente myndigheder samt alle institutter og betalingsinstitutter kunne få udleveret deres individuelle register uden unødigt ophold. Dette register skal omfatte alle outsourcingordninger, herunder outsourcingordninger med tjenesteudbydere i den pågældende koncern eller institutsikringsordning.
  - e. Hvor disse institutter og betalingsinstituttet benytter en exitplan for en kritisk eller vigtig funktion, som er blevet etableret på koncernniveau, i institutsikringsordningen eller af det centrale organ, bør alle institutter og betalingsinstitutter modtage et sammendrag af planen og være overbevist om, at planen kan udføres effektivt.
24. Hvor der er givet dispensation i henhold til artikel 21 i direktiv 2013/36/EU eller artikel 109, stk. 1, i direktiv 2013/36/EU sammenholdt med artikel 7 i forordning (EU) nr. 575/2013, bør bestemmelserne i disse retningslinjer anvendes af moderselskabet i en medlemsstat for sig selv og dets datterselskaber eller af det centrale organ og dets partnere som helhed.
25. Institutter og betalingsinstitutter, der er datterselskaber i et EU-moderselskab eller i et moderselskab i en medlemsstat, som ikke har fået nogen dispensationer i henhold til artikel 21 i direktiv 2013/36/EU eller artikel 109, stk. 1, i direktiv 2013/36/EU sammenholdt med artikel 7 i forordning (EU) nr. 575/2013, bør sikre, at de overholder disse retningslinjer på et individuelt grundlag.

## Del II – Vurdering af outsourcingordninger

### 3 Outsourcing

26. Institutter og betalingsinstitutter bør fastslå, om en ordning med en tredjepart falder ind under definitionen af outsourcing. Inden for denne vurdering bør det overvejes, om den funktion (eller dele heraf), der er outsourcet til en tjenesteudbyder, udføres gentagne gange eller løbende af tjenesteudbyderen, og om denne funktion (eller dele heraf) normalt ville falde inden for rammerne af funktioner, der realistisk set ville eller kunne udføres af institutter eller betalingsinstitutter, også selvom instituttet eller betalingsinstituttet ikke har udført denne funktion selv tidligere.
27. Hvis en ordning med en tjenesteudbyder dækker flere funktioner, bør institutter og betalingsinstitutter overveje alle aspekter af ordningen i deres vurdering. Hvis ydelsen f.eks.

omfatter levering af datalagringshardware og sikkerhedskopiering af data, skal begge aspekter tages i betragtning sammen.

28. Som et generelt princip bør institutter og betalingsinstitutter ikke anse følgende som outsourcing:

- a. en funktion, der er juridisk forpligtet til at blive udført af en tjenesteudbyder, f.eks. lovpligtig revision
- b. markedsinformationstjenester (f.eks. tilvejebringelse af data fra Bloomberg, Moodys, Standard & Poors, Fitch)
- c. globale netværksinfrastrukturer (f.eks. Visa, MasterCard)
- d. clearing og afviklingsordninger mellem clearingcentraler, centrale modparter og afviklingsinstitutter og deres medlemmer
- e. globale finansielle meddelelsesinfrastrukturer, som er underlagt tilsyn af de relevante myndigheder
- f. korrespondentbankydelse og
- g. køb af tjenester, som ellers ikke ville høre under instituttet eller betalingsinstituttet (f.eks. rådgivning fra en arkitekt, juridiske udtalelser og repræsentation for retten og administrative organer, rengøring, havearbejde og vedligeholdelse af instituttets eller betalingsinstituttets lokaler, lægelige ydelser, servicering af firmabiler, catering, automattjenester, funktionærtjenester, rejsetjenester, posttjenester, receptionister, sekretærer og telefonister), varer (f.eks. plastikkort, kortlæsere, kontorartikler, pc'er, møbler) eller forsyning (f.eks. el, gas, vand, telefonlinje).

## 4 Kritiske eller vigtige funktioner

29. Institutter og betalingsinstitutter bør altid anse en funktion som kritisk eller vigtig i følgende situationer:<sup>16</sup>

- a. hvis en fejl eller mangel ved dens udførelse materielt ville forringe:
  - i. deres muligheder for fortsat at overholde betingelserne i deres tilladelse eller øvrige forpligtelser i henhold til direktiv 2013/36/EU, forordning (EU) nr. 575/2013, direktiv 2014/65/EU, direktiv (EU) 2015/2366 og direktiv 2009/110/EF samt deres lovmæssige forpligtelser
  - ii. deres finansielle resultater eller

---

<sup>16</sup> Se også artikel 30 i 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.

- iii. deres mulighed for fortsat eller på et forsvarligt grundlag at yde bank- og betalingstjenester og -aktiviteter
  - b. Hvor operationelle opgaver i interne kontrolfunktioner outsources, medmindre det vurderes, at manglende outsourcing af funktionen eller uhensigtsmæssig outsourcing af funktionen ikke ville have en negativ indvirkning på effektiviteten af den interne kontrolfunktion.
  - c. Hvor de har til hensigt at outsource funktioner inden for bankaktiviteter eller betalingstjenester i et omfang, der ville kræve tilladelse<sup>17</sup> fra en kompetent myndighed som nævnt i afsnit 12.1.
30. I tilfælde af institutter bør der lægges særlig vægt på vurderingen af kritiske eller vigtige funktioner, hvis outsourcingen vedrører funktioner relateret til centrale forretningsområder og kritiske funktioner som defineret i artikel 2, stk. 1, nr. 35), og artikel 2, stk. 1, nr. 36), i direktiv 2014/59/EU<sup>18</sup> og identificeret af institutter, som anvender kriterierne i artikel 6 og 7 i Kommissionens delegerede forordning (EU) 2016/778<sup>19</sup>. Funktioner, som er nødvendige for at udføre opgaver inden for centrale forretningsområder eller kritiske funktioner, bør betragtes som kritiske eller vigtige funktioner med henblik på disse retningslinjer, medmindre instituttet vurderer, at manglende outsourcing af funktionen eller uhensigtsmæssig outsourcing af funktionen ikke ville have en negativ indvirkning på den operationelle kontinuitet i kerneforretningen eller den kritiske funktion.
31. Ved vurderingen af, om en outsourcingordning vedrører en funktion, der er kritisk eller vigtig, bør institutter og betalingsinstitutter sammen med resultatet af vurderingen, som fremgår af afsnit 12.2, som minimum tage højde for følgende faktorer:
- a. om outsourcingordningen er direkte forbundet med levering af de bankaktiviteter eller betalingstjenester<sup>20</sup>, som de har tilladelse til
  - b. de mulige konsekvenser af enhver afbrydelse af den outsourcete funktion eller tjenesteudbyderens manglende evne til at levere tjenesten løbende på det aftalte serviceniveau i forhold til:

---

<sup>17</sup> Se de aktiviteter, der er anført i bilag I til direktiv 2013/36/EU.

<sup>18</sup> Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber og om ændring af Rådets direktiv 82/891/EØF og Europa-Parlamentets og Rådets direktiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU samt Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 af 12.6.2014, s. 190).

<sup>19</sup> Kommissionens delegerede forordning (EU) 2016/778 af 2. februar 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/59/EU for så vidt angår de forhold og betingelser, under hvilke betalingen af ekstraordinære ex post-bidrag helt eller delvis kan udskydes, og kriterierne for fastsættelse af aktiviteter, ydelser og transaktioner med hensyn til kritiske funktioner og for fastsættelse af forretningsområder og hertil knyttede ydelser med hensyn til centrale forretningsområder (EUT L 131 af 20.5.2016, s. 41).

<sup>20</sup> Se de aktiviteter, der er anført i bilag I til direktiv 2013/36/EU.

- i. kort- og langsigtet økonomisk modstandskraft og levedygtighed, herunder, hvis det er relevant, aktiver, kapital, omkostninger, finansiering, likviditet, fortjeneste og tab
  - ii. forretningskontinuitet og operationel modstandskraft
  - iii. operationel risiko, herunder adfærd, informations- og kommunikationsteknologi (IKT) og juridiske risici
  - iv. omdømmemæssige risici
  - v. hvor det er relevant, genopretnings- og afviklingsplanlægning, afviklingsmuligheder og operationel kontinuitet i forbindelse med en situation med tidlig indsats, genopretning eller afvikling
- c. de potentielle konsekvenser af outsourcingordningen for deres evne til at:
  - i. identificere, overvåge og styre alle risici
  - ii. overholde alle juridiske og lovgivningsmæssige krav
  - iii. foretage passende revisioner vedrørende den outsourcete funktion
- d. den potentielle indvirkning på ydelserne til kunderne
- e. alle outsourcingordninger, instituttets eller betalingsinstituttets samlede eksponering for den samme tjenesteudbyder og den potentielle samlede virkning af outsourcingordninger inden for samme forretningsområde
- f. størrelsen og kompleksiteten af de berørte forretningsområder
- g. muligheden for, at den foreslåede outsourcingordning kan opskaleres uden at erstatte eller revidere den underliggende aftale
- h. evnen til at overføre den foreslåede outsourcingordning til en anden tjenesteudbyder, hvis det er nødvendigt eller ønskeligt, både kontraktligt og i praksis, herunder de anslåede risici, hindringer for forretningskontinuiteten, omkostninger og tidsramme herfor ("substituerbarhed")
- i. evnen til at reintegrere den outsourcete funktion i instituttet eller betalingsinstituttet, hvis det er nødvendigt eller ønskeligt
- j. beskyttelse af data og de potentielle konsekvenser af et brud på tavshedspligten eller manglende sikring af tilgængeligheden af data og integritet for instituttet eller betalingsinstituttet og dets kunder, herunder, men ikke begrænset til, overholdelse af forordning (EU) 2016/679<sup>21</sup>.

---

<sup>21</sup> 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 (generelle data beskyttelsesforordning).

## Del III – Ledelsesramme

### 5 Forsvarlige ledelsesordninger og tredjepartsrisiko

32. Som en del af den overordnede ramme for intern kontrol<sup>22</sup>, herunder interne kontrolmekanismer<sup>23</sup>, bør institutter og betalingsinstitutter have en holistisk ramme for risikostyring i hele instituttet, der dækker alle forretningsområder og interne enheder. I henhold til denne ramme bør institutter og betalingsinstitutter afdække og håndtere alle deres risici, herunder risici forårsaget af aftaler med tredjemand. Rammen for risikostyring bør også gøre det muligt for institutter og betalingsinstitutter at træffe velinformerede beslutninger om risikovillighed og sikre, at risikohåndteringsforanstaltninger er behørigt gennemført, herunder med hensyn til cyberrisici<sup>24</sup>.
33. Institutter og betalingsinstitutter bør under hensyntagen til proportionalitetsprincippet i overensstemmelse med afsnit 1 afdække, vurdere, overvåge og styre alle risici, som følger af aftaler med tredjepart, og som de er eller kan blive udsat for, uanset om disse ordninger er outsourcingordninger. Risiciene, især de operationelle risici, for alle ordninger med tredjeparter, herunder dem, der er nævnt i punkt 26 og 28, bør vurderes i overensstemmelse med afsnit 12.2.
34. Institutter og betalingsinstitutter bør sikre, at de overholder alle krav i henhold til forordning (EU) 2016/679, herunder for deres tredjeparts- og outsourcingordninger.

### 6 Forsvarlige ledelsesordninger og outsourcing

35. Outsourcing af funktioner kan ikke medføre delegering af ledelsens ansvar. Institutter og betalingsinstitutter har det fulde ansvar og er ansvarlige for at overholde alle deres forskriftsmæssige forpligtelser, herunder evnen til at føre tilsyn med outsourcing af kritiske eller vigtige funktioner.
36. Ledelsesorganet har til enhver tid det fulde ansvar for som minimum:
- at sikre, at instituttet eller betalingsinstituttet løbende opfylder de betingelser, som det skal opfylde for at bevare sin tilladelse, herunder eventuelle betingelser pålagt af den kompetente myndighed
  - den interne organisation i instituttet eller betalingsinstituttet
  - afdækning, vurdering og styring af interessekonflikter

---

<sup>22</sup> Institutter henvises til del V i EBA's retningslinjer for intern ledelse.

<sup>23</sup> I øvrigt henvises til artikel 11 i direktiv 2015/2366 (det andet betalingstjenestestedirektiv).

<sup>24</sup> Se også EBA's retningslinjer for IKT og sikkerhedsrisikostyring (<https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management>) og G7's grundlæggende elementer for tredjeparts cyberrisikostyring i den finansielle sektor ([https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector\\_en](https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en)).

- d. fastsættelse af instituttets eller betalingsinstituttets strategier og politikker (f.eks. forretningsmodel, risikovillighed, risikostyringsramme)
  - e. tilsyn med den daglige ledelse af instituttet eller betalingsinstituttet, herunder styring af alle risici i forbindelse med outsourcing
  - f. ledelsesorganets tilsynsrolle i dets tilsynsfunktion, herunder tilsyn med og overvågning af ledelsens beslutningstagning.
37. Outsourcing bør ikke sænke egnethedskravet for medlemmerne af et instituts ledelsesorgan, bestyrelsesmedlemmer og personer med ansvar for ledelsen af betalingsinstituttet og personer, der besidder nøgleposter. Institutter og betalingsinstitutter bør have tilstrækkelig kompetence og tilstrækkelige og passende kvalificerede ressourcer til at sikre en hensigtsmæssig styring af og tilsyn med outsourcingordninger.
38. Institutter og betalingsinstitutter bør:
- a. klart fordele ansvaret for dokumentation, styring og kontrol af outsourcingordninger
  - b. afsætte tilstrækkelige ressourcer til at sikre overholdelse af alle juridiske og lovgivningsmæssige krav, herunder disse retningslinjer og dokumentation og overvågning af alle outsourcingordninger
  - c. under hensyntagen til afsnit 1 i disse retningslinjer oprette en outsourcingfunktion eller udpege en højtstående medarbejder, som er direkte ansvarlig over for ledelsesorganet (f.eks. en person, der besidder en nøglepost i en kontrolfunktion) og ansvarlig for styringen og overvågningen af outsourcingordninger som en del af instituttets ramme for intern kontrol og for tilsyn med dokumentationen af outsourcingordninger. Små og mindre komplekse institutter og betalingsinstitutter bør som minimum sikre en klar fordeling af opgaver og ansvar for styringen af og kontrollen med outsourcingordninger og kan tildele outsourcingfunktionen til et medlem af instituttets eller betalingsinstituttets ledelsesorgan.
39. Institutter og betalingsinstitutter bør til enhver tid opretholde tilstrækkelig substans og ikke blive "tomme skaller" eller "skuffeselskaber". Med henblik herpå bør de:
- a. til enhver tid opfylde alle betingelserne i deres tilladelse<sup>25</sup>, herunder en effektiv udøvelse af deres beføjelser gennem ledelsesorganet, jf. punkt 36 i disse retningslinjer

---

<sup>25</sup> Se også de reguleringsmæssige tekniske standarder (RTS) i henhold til artikel 8, stk. 2, i direktiv 2013/36/EU om de oplysninger, der skal forelægges ved ansøgningen om tilladelse til at udøve virksomhed som kreditinstitut, og de gennemførelsesmæssige tekniske standarder (ITS) i henhold til artikel 8, stk. 3, i direktiv 2013/36/EU om standardformularer, -modeller og -procedurer for forelæggelse af de oplysninger, der kræves for at få tilladelse til at udøve virksomhed som kreditinstitut (<https://eba.europa.eu/regulation-and-policy/other-topics/rt-and-its-on-the-authorisation-of-credit-institutions>).

For betalingsinstitutter henvises til EBA's retningslinjer i henhold til direktiv (EU) 2015/2366 (det andet betalingstjenestedirektiv) om de oplysninger, der skal gives for at meddele tilladelse til at udøve virksomhed som

- b. fastholde en klar og gennemsigtig organisatorisk ramme og struktur, der gør dem i stand til at sikre overholdelse af juridiske og forskriftsmæssige krav
- c. hvor operationelle opgaver i interne kontrolfunktioner outsources (f.eks. i tilfælde af koncernintern outsourcing eller outsourcing i institutsikringsordninger) udøve passende tilsyn og være i stand til at styre de risici, der genereres af outsourcing af kritiske eller vigtige funktioner, og
- d. have tilstrækkelige ressourcer og kapacitet til at sikre overholdelse af litra a) til c).

40. I forbindelse med outsourcing bør institutter og betalingsinstitutter som minimum sikre, at:

- a. de kan træffe og gennemføre beslutninger i forbindelse med deres forretningsaktiviteter og kritiske eller vigtige funktioner, herunder med hensyn til dem, der er blevet outsourcet
- b. de opretholder orden i varetagelsen af deres forretning og de bank- og betalingstjenester, de leverer
- c. risici i forbindelse med nuværende og planlagte outsourcingordninger er tilstrækkeligt afdækket, vurderet, styret og begrænset, herunder risici i forbindelse med IKT og finansiel teknologi (fintech)
- d. der er indført passende fortrolighedsordninger med hensyn til data og andre oplysninger
- e. der opretholdes en passende strøm af relevante oplysninger med tjenesteudbydere
- f. de med hensyn til outsourcing af kritiske eller vigtige funktioner er i stand til at foretage mindst én af følgende handlinger inden for en passende tidsramme:
  - i. overføre funktionen til alternative tjenesteudbydere
  - ii. reintegrere funktionen eller
  - iii. afbryde de forretningsmæssige aktiviteter, der er afhængige af funktionen.
- g. hvor personoplysninger behandles af tjenesteudbydere beliggende i EU og/eller tredjelande, der er gennemført relevante foranstaltninger, og data behandles i overensstemmelse med forordning (EU) 2016/679.

## 7 Outsourcingpolitik

41. Ledelsesorganet i et institut eller betalingsinstitut<sup>26</sup>, som har indført outsourcingordninger eller har planer om at indgå sådanne ordninger, bør godkende, regelmæssigt revidere og ajourføre en skriftlig outsourcingpolitik og sikre dens gennemførelse, hvor det er relevant, på et individuelt, delkonsolideret og konsolideret grundlag. For institutter bør outsourcingpolitikken være i overensstemmelse med afsnit 8 i EBA's retningslinjer for intern ledelse og bør især tage hensyn til kravene i afsnit 18 (nye produkter og væsentlige ændringer) af disse retningslinjer. Betalingsinstitutter kan også tilpasse deres politik i forhold til afsnit 8 og 18 i EBA's retningslinjer for intern ledelse.
42. Politikken bør indeholde de vigtigste faser i outsourcingordningers livscyklus og fastlægge principper, ansvar og processer i forbindelse med outsourcing. Politikken bør især som minimum omfatte følgende:
  - a. ledelsesorganets ansvar i overensstemmelse med punkt 36, herunder dets deltagelse, hvor det er relevant, i beslutningsprocessen om outsourcing af afgørende eller væsentlige funktioner
  - b. inddragelse af forretningsområder, interne kontrolfunktioner og andre personer i forbindelse med outsourcingordninger
  - c. planlægning af outsourcingordninger, herunder:
    - i. afdækning af forretningsmæssige krav vedrørende outsourcingordninger
    - ii. kriterier, herunder kriterierne i afsnit 4, og fremgangsmåder til afdækning af kritiske eller vigtige funktioner
    - iii. risikoafdækning, -vurdering og -styring i overensstemmelse med afsnit 12.2
    - iv. kontrol af fornøden omhu for fremtidige tjenesteudbydere, herunder de foranstaltninger, der kræves i henhold til afsnit 12.3
    - v. procedurer for afdækning, vurdering, styring og afhjælpning af potentielle interessekonflikter i overensstemmelse med afsnit 8
    - vi. planlægning af forretningskontinuitet i overensstemmelse med afsnit 9
    - vii. godkendelsesprocessen for nye outsourcingordninger
  - d. gennemførelse, overvågning og styring af outsourcingordninger, herunder:

---

<sup>26</sup> Se også EBA's retningslinjer for sikkerhedsforanstaltninger for operationelle og sikkerhedsmæssige risici for betalingstjenester i henhold til det andet betalingstjenestedirektiv her: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2>



- i. løbende vurdering af tjenesteudbyderens resultater i overensstemmelse med afsnit 14
  - ii. procedurer for at blive underrettet om og reagere på ændringer i en outsourcingordning eller vedrørende en tjenesteudbyder (f.eks. økonomisk stilling, organisatorisk struktur eller ejerstruktur, underoutsourcing)
  - iii. uafhængig gennemgang og revision af overholdelsen af juridiske og forskriftsmæssige krav og politikker
  - iv. fornyelsesprocesser
- e. dokumentation og journalføring, idet der tages hensyn til kravene i afsnit 11
  - f. exitstrategier og opsigelsesprocesser, herunder et krav om en dokumenteret exitplan for hver kritiske eller vigtige funktion, der skal outsources, hvor en sådan exit anses for mulig under hensyntagen til eventuelle driftsafbrydelser eller uventet opsigelse af en outsourcingaftale.

43. I outsourcingpolitikken bør der skelnes mellem følgende:

- a. outsourcing af kritiske eller vigtige funktioner og andre outsourcingordninger
- b. outsourcing til tjenesteudbydere, som er godkendt af en kompetent myndighed, og dem, der ikke er
- c. koncerninterne outsourcingordninger, outsourcingordninger inden for samme institutsikringsordning (herunder enheder, som er ejet 100 % enten individuelt eller kollektivt af institutter i institutsikringsordningen) og outsourcing til enheder uden for koncernen og
- d. outsourcing til tjenesteudbydere, der ligger i en medlemsstat og tredjelande.

44. Institutter og betalingsinstitutter bør sikre, at politikken dækker afdækning af følgende potentielle virkninger af kritiske eller vigtige outsourcingordninger, og at der tages højde for disse i beslutningsprocessen:

- a. instituttets risikoprofil
- b. evnen til at føre tilsyn med tjenesteudbyderen og styre risiciene
- c. forretningskontinuitetsforanstaltninger og
- d. resultaterne af deres forretningsaktiviteter.

## 8 Interessekonflikter

45. I overensstemmelse med del IV, afsnit 11, i EBA's retningslinjer for intern ledelse<sup>27</sup> og betalingsinstitutter bør institutterne afdække, vurdere og håndtere interessekonflikter med hensyn til deres outsourcingordninger.
46. Hvor outsourcing skaber væsentlige interessekonflikter, herunder mellem enheder inden for samme koncern eller institutsikringsordning, skal institutter og betalingsinstitutter træffe passende foranstaltninger til håndtering af de pågældende interessekonflikter.
47. Når funktioner tilvejebringes af en tjenesteudbyder, som er en del af en koncern eller medlem af en institutsikringsordning, eller som ejes af instituttet, betalingsinstituttet, koncernen eller institutter, som er medlemmer af en institutsikringsordning, bør betingelserne, herunder de finansielle betingelser, for den outsourcete tjeneste fastsættes på markedsvilkår. I forbindelse med prisfastsættelse af ydelserne kan der opstå synergier gennem levering af de samme eller lignende ydelser til flere institutter i en koncern eller en institutsikringsordning, så længe tjenesteudbyderen er levedygtig for sig selv. I en koncern bør dette være uafhængigt af, om en anden koncernenhed bliver nødlidende.

## 9 Forretningskontinuitetsplaner

48. Institutter i overensstemmelse med kravene i artikel 85, stk. 2, i direktiv 2013/36/EU og del VI i EBA's retningslinjer for intern ledelse<sup>28</sup>, og betalingsinstitutter skal have indført, vedligeholde og regelmæssigt teste passende forretningskontinuitetsplaner med hensyn til outsourcete kritiske eller vigtige funktioner. Institutter og betalingsinstitutter i en koncern eller institutsikringsordning kan anvende centralt fastlagte forretningskontinuitetsplaner vedrørende deres outsourcete funktioner.
49. I forretningskontinuitetsplaner bør der tages højde for den mulighed, at kvaliteten af de leverede outsourcete kritiske eller vigtige funktioner forringes til et uacceptabelt niveau eller slet ikke lykkes. I sådanne planer bør der også tages højde for den potentielle virkning af insolvens eller andre fejl hos tjenesteudbyderen og, hvor det er relevant, politiske risici i tjenesteudbyderens jurisdiktion.

---

<sup>27</sup> Betalingsinstitutter kan også tilpasse deres politikker til disse retningslinjer.

<sup>28</sup> Tilgængelig under: <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->

## 10 Den interne revisionsfunktion

50. Den interne revisions<sup>29</sup> aktiviteter bør efter en risikobaseret tilgang omfatte en uafhængig gennemgang af outsourcete aktiviteter. Revisionsplanen<sup>30</sup> og -programmet bør især omfatte outsourcingordninger for kritiske eller vigtige funktioner.
51. Med hensyn til outsourcingprocessen bør den interne revisionsfunktion som minimum føre kontrol med:
- at instituttets eller betalingsinstituttets rammer for outsourcing, herunder outsourcingpolitikken, er korrekte og gennemførte og er i overensstemmelse med gældende love og forskrifter, risikostrategien og ledelsesorganets beslutninger
  - tilstrækkeligheden, kvaliteten og effektiviteten af vurderingen af, om funktionerne er kritiske eller vigtige
  - tilstrækkeligheden, kvaliteten og effektiviteten af risikovurderingen for outsourcingordninger, og at risiciene er i overensstemmelse med instituttets risikostrategi
  - at der er passende inddragelse af ledelsesorganer og
  - at der er passende overvågning og styring af outsourcingordninger.

## 11 Dokumentationskrav

52. Som en del af deres risikostyringsrammer bør institutter og betalingsinstitutter opretholde et opdateret register over oplysninger om alle outsourcingordninger i instituttet og, hvor det er relevant, på delkonsolideret og konsolideret plan som beskrevet i afsnit 2, og bør på passende vis dokumentere alle nuværende outsourcingordninger, idet der skelnes mellem outsourcing af kritiske eller vigtige funktioner og andre outsourcingordninger. Under hensyntagen til den nationale lovgivning bør institutter opbevare dokumentation for afsluttede outsourcingordninger i registret og støttedokumentation i en passende periode.
53. Under hensyntagen til del I i disse retningslinjer og på de betingelser, der er fastsat i afsnit 23, litra d), kan registret for institutter og betalingsinstitutter i en koncern, institutter, som er varigt tilknyttet et centralt organ, eller institutter, som er medlemmer af samme institutsikringsordning, føres centralt.

---

<sup>29</sup> Med hensyn til den interne revisions ansvar henvises institutter til afsnit 22 i EBA's retningslinjer for intern ledelse (<https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->) og betalingsinstitutter henvises til retningslinje 5 i EBA's retningslinjer for tilladelser til betalingsinstitutter (<https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf>).

<sup>30</sup> Se også EBA's retningslinjer for tilsyns kontrol- og vurderingsprocessen: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing>

54. Registret skal som minimum indeholde følgende oplysninger for alle eksisterende outsourcingordninger:

- a. et referencenummer for hver outsourcingordning
- b. startdato og, hvor det er relevant, den næste kontraktfornyelsesdato, slutdato og/eller opsigelsesvarsel for tjenesteudbyderen og for instituttet eller betalingsinstituttet
- c. en kort beskrivelse af den outsourcede funktion, herunder de data, der er outsourcet, og om der er overført persondata (f.eks. ved angivelse af ja eller nej i et særskilt felt), eller om behandlingen heraf er outsourcet til en tjenesteudbyder
- d. en kategori tildelt af instituttet eller betalingsinstituttet, der afspejler karakteren af funktionen som beskrevet under litra c), (f.eks. informationsteknologi (IT), kontrolfunktion), hvilket bør gøre det lettere at identificere de forskellige typer ordninger
- e. navnet på tjenesteudbyderen, selskabets registreringsnummer, den juridiske enheds id (hvor det er tilgængeligt), den registrerede adresse og andre relevante kontaktoplysninger og navnet på moderselskabet (evt.)
- f. det land eller de lande, hvor serviceydelsen skal udføres, herunder datalokaliseringen (dvs. land eller region)
- g. hvorvidt (ja/nej) den outsourcede funktion betragtes som kritisk eller vigtig, herunder i givet fald et kort sammendrag af grundene til, at den outsourcede funktion betragtes som kritisk eller vigtig
- h. i tilfælde af outsourcing til en udbyder af cloudtjenester den pågældende cloudtjeneste og implementeringsmodellerne, dvs. offentlig/privat/hybrid/fælles cloud, og den særlige karakter af de data, der skal opbevares, samt de lokaliteter (dvs. lande eller regioner), hvor sådanne data vil blive opbevaret
- i. datoen for den seneste vurdering af, om den outsourcede funktion er afgørende eller væsentlig.

55. For outsourcing af kritiske eller vigtige funktioner bør registret som minimum indeholde følgende yderligere oplysninger:

- a. institutter, betalingsinstitutter og andre virksomheder, der er omfattet af den tilsynsmæssige konsolidering eller institutsikringsordningen, hvor det er relevant, og som gør brug af outsourcing
- b. hvorvidt tjenesteudbyderen eller underleverandøren er en del af koncernen eller medlem af institutsikringsordningen eller er ejet af institutter eller betalingsinstitutter i koncernen eller er ejet af medlemmer af en institutsikringsordning

- c. datoen for den seneste risikovurdering og en kort oversigt over de vigtigste resultater
  - d. den person eller det beslutningsorgan (f.eks. ledelsesorgan) i instituttet eller betalingsinstituttet, som godkendte outsourcingordningen
  - e. den gældende lovgivning for outsourcingordningen
  - f. datoerne for de seneste og næste planlagte revisioner, hvor det er relevant
  - g. hvis det er relevant, navnene på eventuelle underleverandører, som væsentlige dele af en kritisk eller vigtig funktion er underoutsourcet til, herunder det land, hvor underleverandørerne er registreret, hvor ydelsen vil blive udført, og, hvis det er relevant, den lokalitet (dvs. land eller region), hvor dataene skal opbevares
  - h. et resultat af vurderingen af tjenesteudbyderens substituerbarhed (let, vanskelig eller umulig), muligheden for at reintegrere en kritisk eller vigtig funktion i instituttet eller betalingsinstituttet eller virkningen af, at den kritiske eller vigtige funktion ophører
  - i. afdækning af alternative tjenesteudbydere i overensstemmelse med litra h)
  - j. hvorvidt de outsourcete kritiske eller vigtige funktioner understøtter en tidskritisk forretningsdrift
  - k. de anslåede årlige budgetomkostninger.
56. Institutter og betalingsinstitutter bør på anmodning stille enten det fulde register over alle eksisterende outsourcingordninger<sup>31</sup> eller de ovenfor anførte afsnit såsom oplysninger om alle outsourcingordninger, der falder ind under én af de kategorier, der er nævnt i punkt 54, litra d), i disse retningslinjer (f.eks. alle IT-outsourcingordninger) til rådighed for den kompetente myndighed. Institutter og betalingsinstitutter bør tilvejebringe disse oplysninger i en elektronisk læsbar form (f.eks. et almindeligt anvendt databaseformat, kommaseparerede værdier).
57. Institutter og betalingsinstitutter bør på anmodning stille alle nødvendige oplysninger til rådighed for den kompetente myndighed, som denne skal bruge til at udføre et effektivt tilsyn med instituttet eller betalingsinstituttet, herunder, hvis det er nødvendigt, en kopi af outsourcingaftalen.
58. Uden at det berører artikel 19, stk. 6, i direktiv (EU) 2015/2366, bør institutter og betalingsinstitutter på passende vis informere de kompetente myndigheder i tide eller deltage i en dialog om tilsyn med de kompetente myndigheder om den planlagte outsourcing af kritiske

---

<sup>31</sup> I øvrigt henvises til EBA's retningslinjer for tilsynskontrol og vurderingsprocessen, som findes her: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

eller vigtige funktioner og/eller som minimum give de oplysninger, som fremgår af punkt 54, når en outsourcet funktion er blevet kritisk eller vigtig.

59. Institutter og betalingsinstitutter<sup>32</sup> bør informere de kompetente myndigheder i tide om væsentlige ændringer og/eller alvorlige hændelser vedrørende deres outsourcingordninger, der kan have en væsentlig indvirkning på den fortsatte levering af instituttets eller betalingsinstituttets forretningsaktiviteter.
60. Institutter og betalingsinstitutter bør på passende vis dokumentere vurderingerne i henhold til afsnit IV og resultaterne af deres løbende overvågning (f.eks. tjenesteudbyderens tjenester, overholdelse af aftalte serviceniveauer, andre kontraktlige og forskriftsmæssige krav, opdateringer til risikovurderingen).

## Del IV – Outsourcingproces

### 12 Analyse inden outsourcing

61. Inden institutter og betalingsinstitutter indgår i en outsourcingordning, bør de:
- vurdere, om outsourcingordningen vedrører en kritisk eller vigtig funktion som fastsat i del II
  - vurdere, om tilsynsbetingelserne for outsourcing i afsnit 12.1 er opfyldt
  - afdække og vurdere alle de relevante risici ved outsourcingordningen i overensstemmelse med afsnit 12.2
  - anvende en due diligence-procedure i forhold til den potentielle tjenesteudbyder i overensstemmelse med afsnit 12.3
  - afdække og vurdere de interessekonflikter, som outsourcing kan forårsage i overensstemmelse med afsnit 8.

#### 12.1 Tilsynsbetingelser for outsourcing

62. Institutter og betalingsinstitutter bør sikre outsourcing af funktioner inden for bankaktiviteter<sup>33</sup> eller betalingstjenester, for så vidt at udførelsen af den pågældende funktion kræver tilladelse eller registrering hos en kompetent myndighed i den medlemsstat, hvor de er godkendt, til en tjenesteudbyder med hjemsted i den samme eller en anden medlemsstat kun finder sted, hvis en af følgende betingelser er opfyldt:

---

<sup>32</sup> Se også EBA's retningslinjer for indberetning af større hændelser i henhold til det andet betalingstjenestedirektiv, som findes her: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

<sup>33</sup> Se artikel 9 i kapitalkravsdirektivet om forbud for personer eller andre virksomheder end kreditinstitutter mod erhvervsmæssigt at tage imod indskud eller andre tilbagebetalingspligtige midler fra offentligheden.

- a. tjenesteudbyderen er godkendt eller registreret af en kompetent myndighed til at udføre sådanne bankaktiviteter eller betalingstjenester eller
- b. tjenesteudbyderen har på anden vis tilladelse til at udføre disse bankaktiviteter eller betalingstjenester i overensstemmelse med den relevante nationale rammelovgivning.

63. Institutter og betalingsinstitutter bør sikre, at outsourcing af funktioner inden for bankaktiviteter eller betalingstjenester, for så vidt at udførelsen af den pågældende funktion kræver tilladelse eller registrering hos en kompetent myndighed i den medlemsstat, hvor er godkendt, til en tjenesteudbyder med hjemsted i et tredjeland kun finder sted, hvis en af følgende betingelser er opfyldt:

- a. tjenesteudbyderen har tilladelse eller er registreret til at levere den pågældende bankaktivitet eller betalingstjeneste i tredjelandet og er underlagt tilsyn fra en relevant kompetent myndighed i det pågældende tredjeland ("tilsynsmyndighed")
- b. der foreligger en passende samarbejdsaftale, f.eks. i form af et aftalememorandum eller en samarbejdsaftale mellem de kompetente myndigheder med ansvar for tilsynet med instituttet, og tilsynsmyndighederne med ansvar for tilsynet med tjenesteudbyderen, og
- c. samarbejdsaftalen, der er nævnt i litra b), bør sikre, at de kompetente myndigheder som minimum er i stand til:
  - i. på anmodning at indhente de nødvendige oplysninger til at udføre deres tilsynsopgaver i henhold til direktiv 2013/36/EU, forordning (EU) nr. 575/2013, direktiv (EU) 2015/2366 og direktiv 2009/110/EF
  - ii. få passende adgang til alle data, dokumenter, lokaler eller ansatte i et tredjeland, som er relevante for udførelsen af deres tilsynsbeføjelser
  - iii. så hurtigt som muligt modtage oplysninger fra tilsynsmyndigheden i tredjelandet for at undersøge tilsyneladende brud på kravene i direktiv 2013/36/EU, forordning (EU) nr. 575/2013, direktiv (EU) 2015/2366 og direktiv 2009/110/EF og
  - iv. samarbejde med de relevante tilsynsmyndigheder i tredjelandet om håndhævelse i tilfælde af overtrædelse af de gældende myndighedskrav og den nationale lovgivning i medlemsstaten. Samarbejdet bør omfatte, men ikke nødvendigvis være begrænset til, så snart det er praktisk muligt, at modtage oplysninger om potentielle overtrædelser af de gældende krav fra tilsynsmyndighederne i tredjelandet.

## 12.2 Risikovurdering af outsourcingordninger

64. Institutter og betalingsinstitutter bør vurdere de potentielle konsekvenser af outsourcingordninger for deres operationelle risiko, bør tage hensyn til vurderingsresultaterne, når de beslutter, om funktionen skal outsources til en tjenesteudbyder, og bør træffe passende foranstaltninger for at undgå unødige yderligere operationelle risici, før de indgår outsourcingordninger.
65. Vurderingen bør, hvor det er relevant, omfatte scenarier af mulige risikohændelser, herunder meget alvorlige operationelle risikohændelser. I analysen af scenarierne bør institutter og betalingsinstitutter vurdere de potentielle konsekvenser af mislykkede eller utilstrækkelige ydelser, herunder de risici, som processer, systemer, personer eller eksterne begivenheder forårsager. Institutter og betalingsinstitutter bør under hensyntagen til proportionalitetsprincippet, der er nævnt i afsnit 1, dokumentere den udførte analyse og deres resultater og bør vurdere, i hvilket omfang outsourcingordningen ville øge eller mindske deres operationelle risiko. Under hensyntagen til afsnit I kan små og ikkekomplekse institutter og betalingsinstitutter bruge kvalitative metoder til risikovurdering, mens store eller komplekse institutter bør have en mere sofistikeret tilgang, herunder eventuelt brug af interne og eksterne tabsdata i analysen af scenarier.
66. I forbindelse med risikovurderingen bør institutter og betalingsinstitutter også tage hensyn til de forventede fordele og omkostninger ved den foreslåede outsourcingordning, herunder vægte risici, der kan reduceres eller styres bedre i forhold til risici, der kan opstå som følge af den foreslåede outsourcingordning under hensyntagen til som minimum:
- a. koncentrationsrisici, herunder fra:
    - i. outsourcing til en dominerende tjenesteudbyder, der ikke er let substituerbar, og
    - ii. flere outsourcingordninger med den samme tjenesteudbyder eller nært forbundne tjenesteudbydere
  - b. de samlede risici som følge af outsourcing af flere funktioner på tværs af instituttet eller betalingsinstituttet og i tilfælde af grupper af institutter eller institutsikringsordninger de samlede risici på et konsolideret grundlag eller på basis af institutsikringsordningen
  - c. i tilfælde af væsentlige institutter er den såkaldte "step-in"-risiko risikoen for at skulle yde økonomisk støtte til en tjenesteudbyder i nød eller overtage dennes forretningsmæssige aktiviteter, og
  - d. de foranstaltninger, som gennemføres af instituttet og betalingsinstituttet og af tjenesteudbyderen med henblik på at styre og mindske risiciene.



67. Hvor outsourcingordningen omfatter muligheden for, at tjenesteudbydere underoutsourcer kritiske eller vigtige funktioner til andre tjenesteudbydere, bør institutter og betalingsinstitutter tage hensyn til:

- a. de risici, der er forbundet med underoutsourcing, herunder de yderligere risici, der kan opstå, hvis underleverandøren er beliggende i et tredjeland eller et andet land end tjenesteudbyderen
- b. risikoen for, at lange og komplekse kæder af underoutsourcing mindsker institutters eller betalingsinstitutters mulighed for at føre tilsyn med outsourcete kritiske eller vigtige funktioner og de kompetente myndigheders evne til effektivt at overvåge dem.

68. Ved gennemførelsen af risikovurderingen forud for outsourcing og under den løbende overvågning af tjenesteudbyderens resultater bør institutter og betalingsinstitutter som minimum:

- a. afdække og klassificere de relevante funktioner og beslægtede data og systemer ud fra følsomhed og påkrævede beskyttelsesforanstaltninger
- b. foretage en grundig risikobaseret analyse af funktionerne og relaterede data og systemer, der er under overvejelse med hensyn til outsourcing eller er blevet outsourcet, og håndtere potentielle risici, især de operationelle risici, herunder juridiske risici, IKT-risici, compliancerisici og omdømmemæssige risici, og de tilsynsmæssige begrænsninger i relation til de lande, hvor de outsourcete ydelser leveres eller kan leveres, og hvor data er eller sandsynligvis vil blive opbevaret
- c. overveje konsekvenserne af tjenesteudbyderens lokalitet (i eller uden for EU)
- d. overveje den politiske stabilitet og sikkerhedssituationen i de pågældende jurisdiktioner, herunder:
  - i. gældende lovgivning, herunder lovgivning om databeskyttelse
  - ii. gældende retshåndhævende bestemmelser og
  - iii. insolvensretlige bestemmelser, som finder anvendelse i tilfælde af en tjenesteudbyders svigt og eventuelle begrænsninger, der vil opstå i forbindelse med den presserende genopretning af instituttets eller betalingsinstituttets data i særdeleshed
- e. definere og fastlægge et passende beskyttelsesniveau for datafortroligheden, kontinuiteten af de outsourcete aktiviteter og integriteten og sporbarheden af dataene og systemerne i forbindelse med den tilsigtede outsourcing. Institutter og betalingsinstitutter 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

- f. overveje, om tjenesteudbyderen er et datterselskab eller moderselskab for instituttet, er omfattet af regnskabskonsolideringen eller er medlem eller ejes af institutter, som er medlemmer af en institutsikringsordning og i givet fald, i hvilket omfang instituttet styrer den eller har mulighed for at påvirke dens handlinger i overensstemmelse med afsnit 2.

## 12.3 Fornøden omhu

- 69. Inden institutter og betalingsinstitutter indgår en outsourcingordning og overvejer de operationelle risici i forbindelse med den funktion, der skal outsources, skal de i forbindelse med valget og vurderingen sikre, at tjenesteudbyderen er egnet.
- 70. Med hensyn til kritiske eller vigtige funktioner bør institutter og betalingsinstitutter sikre, at tjenesteudbyderen har et forretningsområde, passende og tilstrækkelige evner, ekspertise, kapacitet, ressourcer (f.eks. menneskelige, IT-mæssige, finansielle), den organisatoriske struktur og, hvis det er relevant, den eller de krævede myndighedstilladelser eller registreringer til at udføre den kritiske eller vigtige funktion på en pålidelig og professionel måde i forhold til at opfylde sine forpligtelser i hele kontraktudkastets varighed.
- 71. Yderligere faktorer, der skal overvejes, når der foretages en undersøgelse af fornøden omhu for en potentiel tjenesteudbyder, omfatter, men er ikke begrænset til:
  - a. forretningsmodel, art, omfang, kompleksitet, finansiell situation, ejerskab og koncernstruktur
  - b. de langsigtede relationer med tjenesteudbydere, som allerede er vurderet og udfører tjenester for instituttet eller betalingsinstituttet
  - c. om tjenesteudbyderen er et moderselskab eller datterselskab af instituttet eller betalingsinstituttet, indgår i instituttets regnskabsmæssige konsolidering eller er medlem eller ejet af institutter, som er medlemmer af samme institutsikringsordning, som instituttet tilhører
  - d. hvorvidt tjenesteudbyderen er underlagt de kompetente myndigheders tilsyn.
- 72. Hvor outsourcing indebærer behandling af personoplysninger eller fortrolige data, bør institutter og betalingsinstitutter kontrollere, at tjenesteudbyderen træffer passende tekniske og organisatoriske foranstaltninger til at beskytte dataene.
- 73. Institutter og betalingsinstitutter bør tage passende skridt til at sikre, at tjenesteudbydere handler i overensstemmelse med deres værdier og adfærdskodeks. Især med hensyn til tjenesteudbydere i tredjelande og, hvor det er relevant, deres underleverandører, bør institutter og betalingsinstitutter kontrollere, at tjenesteudbyderen handler på en etisk og socialt ansvarlig måde og efterlever internationale standarder for menneskerettigheder (f.eks.

den europæiske menneskerettighedskonvention), miljøbeskyttelse og sikrer passende arbejdsbetingelser, herunder forbud mod børnearbejde.

## 13 Kontraktfase

74. Institutts, betalingsinstitutts og tjenesteudbyderens rettigheder og forpligtelser bør klart fordeles og fastlægges i en skriftlig aftale.

75. Outsourcingaftalen om kritiske eller vigtige funktioner bør som minimum indeholde:

- a. en klar beskrivelse af den outsourcete funktion, der skal leveres
- b. startdato og slutdato, hvor det er relevant, for aftalen og opsigelsesfrister for tjenesteudbyderen og instituttet eller betalingsinstitut
- c. den gældende lovgivning for aftalen
- d. parternes finansielle forpligtelser
- e. hvorvidt det er tilladt at underoutsourcere en kritisk eller vigtig funktion eller væsentlige dele deraf og i bekræftende fald de betingelser i afsnit 13.1, som underoutsourcingen er underlagt
- f. den eller de lokaliteter (dvs. regioner eller lande), hvor den kritiske eller vigtige funktion vil blive leveret, og/eller hvor relevante data vil blive opbevaret og behandlet, herunder den mulige opbevaringslokalitet og de betingelser, som skal opfyldes, herunder et krav om at underrette instituttet eller betalingsinstitut, hvis tjenesteudbyderen foreslår at ændre lokaliteten
- g. hvor det er relevant, bestemmelser om adgang, tilgængelighed, integritet, databeskyttelse og sikkerhed med hensyn til de relevante data som anført i afsnit 13.2
- h. instituttets eller betalingsinstitutts ret til at overvåge tjenesteudbyderens resultater løbende
- i. de aftalte serviceniveauer, som bør omfatte præcise kvantitative og kvalitative resultatmål for den outsourcete funktion for at give mulighed for rettidig overvågning, så der kan træffes passende korrigerende foranstaltninger uden unødigt forsinkelse, hvis de aftalte serviceniveauer ikke overholdes
- j. tjenesteudbyderens indberetningsforpligtelse til instituttet eller betalingsinstitut, herunder tjenesteudbyderens formidling af enhver udvikling, der kan have en væsentlig indflydelse på tjenesteudbyderens evne til effektivt at udføre den kritiske eller vigtige funktion i overensstemmelse med det aftalte serviceniveau og i overensstemmelse med gældende love og myndighedskrav og, hvor det er relevant, forpligtelserne til at indsende rapporter om tjenesteudbyderens interne revisionsfunktion

- k. om tjenesteudbyderen bør tegne obligatorisk forsikring mod visse risici og, hvis det er relevant, omfanget af den ønskede forsikringsdækning
- l. kravene til at gennemføre og teste forretningsberedskabsplaner
- m. bestemmelser, der sikrer, at de data, der ejes af instituttet eller betalingsinstituttet, kan tilgås i tilfælde af insolvens, afvikling eller ophør af tjenesteudbyderens forretningsaktiviteter
- n. tjenesteudbyderens forpligtelse til at samarbejde med de kompetente myndigheder og afviklingsmyndighederne for instituttet eller betalingsinstituttet, herunder andre personer udpeget af disse
- o. for institutter en klar henvisning til den nationale afviklingsmyndigheds beføjelser, især til artikel 68 og 71 i direktiv 2014/59/EU (BRRD) og især en beskrivelse af de "materielle forpligtelser" i kontrakten i henhold til artikel 68 i nævnte direktiv
- p. institutters, betalingsinstitutters og kompetente myndigheders ubegrænsede ret til at inspicere og revidere tjenesteudbyderen med hensyn til især den kritiske eller vigtige outsourcete funktion som angivet i afsnit 13.3
- q. opsigelsesrettigheder som beskrevet i afsnit 13.4.

### 13.1 Underoutsourcing af kritiske eller vigtige funktioner

- 76. Outsourcingaftalen bør angive, om underoutsourcing af kritiske eller vigtige funktioner eller væsentlige dele deraf er tilladt.
- 77. Hvis underoutsourcing af kritiske eller vigtige funktioner er tilladt, bør institutter og betalingsinstitutter afgøre, om den del af funktionen, som skal underoutsources, som sådan er kritisk eller vigtig (dvs. en væsentlig del af den kritiske eller vigtige funktion), og i givet fald optage den i registret.
- 78. Hvis underoutsourcing af kritiske eller vigtige funktioner er tilladt, bør den skriftlige aftale:
  - a. angive eventuelle typer af aktiviteter, der er udelukket fra underoutsourcing
  - b. angive de betingelser, der skal opfyldes i tilfælde af underoutsourcing
  - c. angive, at tjenesteudbyderen er forpligtet til at føre tilsyn med de ydelser, som denne har underoutsourcet, for at sikre, at alle kontraktlige forpligtelser mellem tjenesteudbyderen og instituttet eller betalingsinstituttet løbende er opfyldt

- d. pålægge tjenesteudbyderen at indhente en forudgående specifik eller generel skriftlig tilladelse fra instituttet eller betalingsinstituttet, inden dataene underoutsources<sup>34</sup>
- e. omfatte en forpligtelse for tjenesteudbyderen til at underrette instituttet eller betalingsinstituttet om planlagt underoutsourcing eller væsentlige ændringer deraf, navnlig når dette kan påvirke tjenesteudbyderens evne til at opfylde sine forpligtelser i henhold til outsourcingaftalen. Dette omfatter planlagte væsentlige ændringer vedrørende underleverandører og underretningsperioden. Især bør underretningsperioden give outsourcinginstituttet eller betalingsinstituttet mulighed for som minimum at foretage en risikovurdering af de foreslåede ændringer og gøre indvendinger mod ændringer, før den planlagte underoutsourcing eller væsentlige ændringer heraf træder i kraft
- f. hvor det er relevant sikre, at instituttet eller betalingsinstituttet har ret til at modsætte sig den planlagte underoutsourcing eller væsentlige ændringer deraf, eller at der kræves en udtrykkelig godkendelse
- g. sikre, at instituttet eller betalingsinstituttet har en kontraktlig ret til at opsige aftalen i tilfælde af unødigt underoutsourcing, f.eks. hvor underoutsourcing væsentligt øger risikoen for instituttet eller betalingsinstituttet, eller hvor tjenesteudbyderen underoutsourcer uden at underrette instituttet eller betalingsinstituttet.

79. Institutter og betalingsinstitutter bør acceptere kun at underoutsourcere, hvis underleverandøren forpligter sig til at:

- a. overholde alle gældende love, myndighedskrav og kontraktlige forpligtelser og
- b. give instituttet, betalingsinstituttet og den kompetent myndighed de samme kontraktlige rettigheder til adgang og revision som dem, der ydes af tjenesteudbyderen.

80. Institutter og betalingsinstitutter bør sikre, at tjenesteudbyderen på passende vis fører tilsyn med underleverandører i overensstemmelse med den politik, som er defineret af instituttet eller betalingsinstituttet. Hvis den foreslåede underoutsourcing kunne have væsentlige negative virkninger på outsourcingordningerne for en kritisk eller vigtig funktion eller ville føre til en væsentlig forøgelse af risikoen, herunder hvis betingelserne i punkt 79 ikke ville blive opfyldt, bør instituttet eller betalingsinstituttet udøve sin ret til at modsætte sig underoutsourcing, hvis en sådan ret blev aftalt, og/eller opsige kontrakten.

## 13.2 Data- og systemsikkerhed

81. Institutter og betalingsinstitutter bør sikre, at tjenesteudbydere, hvor det er relevant, opfylder relevante IT-sikkerhedsstandarder.

---

<sup>34</sup> Se artikel 28 i forordning (EU) nr. 2016/679.

82. Hvor det er relevant (f.eks. i forbindelse med cloud- eller anden IKT-outsourcing), bør institutter og betalingsinstitutter definere data- og systemsikkerhedskrav inden for outsourcingaftalen og overvåge overholdelsen af disse krav løbende.
83. I tilfælde af outsourcing til cloududbydere og andre outsourcingordninger, der involverer behandling eller videregivelse af personoplysninger eller fortrolige data, bør institutter og betalingsinstitutter vedtage en risikobaseret tilgang til datalagrings- og databehandlingslokaliteter (dvs. land eller region) og informationssikkerhedshensyn.
84. Med forbehold af kravene i forordning (EU) 2016/679 bør institutter og betalingsinstitutter, når de outsourcer (især til tredjelande), tage hensyn til forskelle i nationale bestemmelser om beskyttelse af data. Institutter og betalingsinstitutter bør sikre, at outsourcingaftalen indeholder en forpligtelse til, at tjenesteudbyderen beskytter fortrolige, personlige eller på anden måde følsomme oplysninger og overholder alle lovkrav med hensyn til beskyttelse af data, der gælder for instituttet eller betalingsinstituttet (f.eks. beskyttelse af personoplysninger og at bankhemmeligheder eller lignende juridisk tavshedspligt med hensyn til kunders oplysninger, hvor det er relevant, er overholdt).

### 13.3 Ret til adgang, oplysninger og revision

85. Institutter og betalingsinstitutter bør inden for den skriftlige outsourcingordning sikre, at den interne revisionsfunktion er i stand til at gennemgå den outsourcete funktion ved hjælp af en risikobaseret tilgang.
86. Uanset hvor kritisk eller vigtig den outsourcete funktion er, bør de skriftlige outsourcingordninger mellem institutter og tjenesteudbydere henvise til de kompetente myndigheders og afviklingsmyndigheders indsamling af oplysninger og undersøgelsesbeføjelser i henhold til artikel 63, stk. 1, litra a), i direktiv 2014/59/EU og artikel 65, stk. 3, i direktiv 2013/36/EU med hensyn til tjenesteudbydere, som er etableret i en medlemsstat, og bør også sikre disse rettigheder med hensyn til tjenesteudbydere i tredjelande.
87. Med hensyn til outsourcing af kritiske eller vigtige funktioner bør institutter og betalingsinstitutter i den skriftlige outsourcingaftale sikre, at tjenesteudbyderen giver dem og deres kompetente myndigheder, herunder afviklingsmyndigheder, og enhver anden person, der er udpeget af dem eller de kompetente myndigheder, følgende:
  - a. fuld adgang til alle relevante forretningslokaler (f.eks. hovedkontorer og driftscentre), herunder hele spektret af relevante enheder, systemer, netværk, oplysninger og data, der anvendes til at levere den outsourcete funktion, herunder relevante finansielle oplysninger, personale og tjenesteudbyderens eksterne revisorer ("ret til adgang og oplysninger"), og

- b. ubegrænset ret til inspektion og revision i forbindelse med outsourcingordningen ("ret til revision") for at sætte dem i stand til at overvåge outsourcingordningen og sikre overholdelse af alle gældende myndighedskrav og kontraktmæssige krav.
88. Ved outsourcing af funktioner, der ikke er kritiske eller vigtige, bør institutter og betalingsinstitutter sikre ret til adgang og revision som anført i punkt 87, litra a) og b), og afsnit 13.3 i en risikobaseret tilgang under hensyntagen til arten af den outsourcete funktion og de dermed forbundne operationelle og omdømmemæssige risici, dens skalerbarhed, den potentielle indvirkning på den fortsatte udførelse af opgaverne og kontraktperioden. Institutter og betalingsinstitutter bør tage højde for, at funktioner kan blive kritiske eller vigtige over tid.
89. Institutter og betalingsinstitutter bør sikre, at outsourcingaftalen eller en anden kontraktordning ikke hindrer eller begrænser den faktiske udøvelse af retten til adgang og revision for dem, de kompetente myndigheder eller en tredjepart udpeget af dem til at udøve disse rettigheder.
90. Institutter og betalingsinstitutter bør udøve deres ret til adgang og revision, fastlægge revisionshyppigheden og områder, der skal revideres, ud fra en risikobaseret tilgang og overholde relevante, almindeligt accepterede, nationale og internationale revisionsstandarder<sup>35</sup>.
91. Uden at det berører deres endelige ansvar med hensyn til outsourcingordninger, kan institutter og betalingsinstitutter anvende:
- a. revisioner i puljer, der tilrettelægges i fællesskab med andre kunder hos den samme tjenesteudbyder, og som udføres af dem og 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 tjenesteudbyderen.
  - b. tredjepartscertificeringer og tredjepartsrevisionsrapporter eller interne revisionsrapporter, der stilles til rådighed af tjenesteudbyderen.
92. Med hensyn til outsourcing af kritiske eller vigtige funktioner bør institutter og betalingsinstitutter vurdere, om tredjepartscertificeringer og tredjepartsrapporter, der er omhandlet i punkt 91, litra b), er passende og tilstrækkelige til at opfylde deres forskriftsmæssige forpligtelser og bør ikke udelukkende forlade sig på disse rapporter over tid.
93. Institutter og betalingsinstitutter bør kun gøre brug af den metode, der er nævnt i punkt 91, litra b), hvis de:
- a. er tilfredse med revisionsplanen for den outsourcete funktion

---

<sup>35</sup> Institutter henvises til afsnit 2.2 i EBA's retningslinjer for intern ledelse: <https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889>



- b. sikrer, at anvendelsesområdet for certificeringen eller revisionsrapporten omfatter de systemer (dvs. processer, applikationer, infrastruktur, datacentre mv.) og nøglekontroller, som instituttet eller betalingsinstituttet har udpeget, samt overholdelse af relevante myndighedskrav
- c. grundigt vurderer indholdet af certificeringerne eller revisionsrapporterne løbende og kontrollerer, at rapporterne eller certificeringerne ikke er forældede
- d. sikrer, at centrale systemer og kontroller indgår i fremtidige versioner af certificeringen eller revisionsrapporten
- e. 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)
- f. er overbevist om, at certificeringerne udstedes, og revisionerne udføres i henhold til anerkendte relevante branchestandarder og indbefatter en test af de vigtigste eksisterende kontrollers operationelle effektivitet
- g. har kontraktlig ret til at anmode om, at certificeringernes eller revisionsrapporternes anvendelsesområde udvides til andre relevante systemer og kontroller; antallet og hyppigheden af disse anmodninger om ændring af anvendelsesområdet bør være rimelige og berettigede ud fra et risikostyringsperspektiv, og
- h. bevarer den kontraktmæssige ret til at udføre individuelle revisioner efter eget skøn med hensyn til outsourcing af kritiske eller vigtige funktioner.

94. I overensstemmelse med EBA's retningslinjer for IKT-risikovurdering under tilsyns kontrol- og vurderingsprocessen (SREP) bør institutter, hvor det er relevant, sikre, at de er i stand til at udføre test af sikkerhedsbrister for at vurdere effektiviteten af de gennemførte cyber- og interne IKT-sikkerhedsforanstaltninger <sup>36</sup>. Under hensyntagen til del I bør betalingsinstitutter også have interne IKT-kontrolmekanismer, herunder IKT-sikkerhedskontrol og afhjælpende foranstaltninger.

95. Før et planlagt besøg på stedet bør institutter, betalingsinstitutter, kompetente myndigheder og revisorer eller tredjeparter, der handler på vegne af instituttet, betalingsinstituttet eller de kompetente myndigheder, give tjenesteudbyderen et rimeligt varsel, medmindre dette ikke er muligt på grund af en nødsituation eller krisesituation eller ville føre til en situation, hvor revisionen ikke længere vil være effektiv.

---

<sup>36</sup> Se også EBA's retningslinjer for IKT-risiko: <https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a>

96. Når der udføres revisioner i miljøer med flere kunder, skal det sikres, at en anden kundes miljø ikke udsættes for risici (f.eks. indvirkning på serviceniveauet, datatilgængelighed, fortrolighedsaspekter), eller at sådanne risici mindskes.
97. Hvor outsourcingordningen indebærer en høj grad af teknisk kompleksitet, f.eks. i tilfælde af cloudoutsourcing, bør instituttet eller betalingsinstituttet kontrollere, at den, der udfører revisionen – uanset om det er de interne revisorer, puljen af revisorer eller eksterne revisorer, der handler på deres vegne – har hensigtsmæssige og relevante færdigheder og viden til at udføre relevante revisioner og/eller vurderinger effektivt. Det samme gælder for alle ansatte i instituttet eller betalingsinstituttet, som gennemgår tredjepartscertificeringer eller revisioner udført af tjenesteudbydere.

### 13.4 Ret til opsigelse

98. Outsourcingordningen bør udtrykkeligt give mulighed for, at instituttet eller betalingsinstituttet kan opsiges ordningen i overensstemmelse med gældende ret, herunder i følgende situationer:
- a. Hvor tjenesteudbyderen af de outsourcede funktioner overtræder gældende love, forskrifter eller kontraktmæssige bestemmelser.
  - b. Hvor der er hindringer, som kan ændre resultatet af den outsourcede funktion.
  - c. Hvor der er væsentlige ændringer, der påvirker outsourcingordningen eller tjenesteudbyderen (f.eks. underoutsourcing eller ændringer af underleverandører).
  - d. Hvor der er svagheder med hensyn til forvaltningen og sikkerheden af fortrolige, personlige eller på anden måde følsomme data og oplysninger.
  - e. Hvor instituttets eller betalingsinstituttets kompetente myndighed giver instrukser, f.eks. i tilfælde af, at den kompetente myndighed som følge af outsourcingordningen ikke længere er i stand til effektivt at overvåge instituttet eller betalingsinstituttet.
99. Outsourcingordningen bør lette overføringen af den outsourcede funktion til en anden tjenesteudbyder eller genindføre den i instituttet eller betalingsinstituttet. Til dette formål bør den skriftlige outsourcingordning:
- a. klart beskrive den eksisterende tjenesteudbyders forpligtelser, hvis den outsourcede funktion overføres til en anden tjenesteudbyder eller tilbage til instituttet eller betalingsinstituttet, herunder behandling af data
  - b. fastsætte en passende overgangsperiode, hvor tjenesteudbyderen efter afslutningen af outsourcingordningen vil fortsætte med at levere den outsourcede funktion for at reducere risikoen for forstyrrelser, og

- c. indeholde en forpligtelse for tjenesteudbyderen til at støtte instituttet eller betalingsinstituttet gennem en korrekt overføring af funktionen, såfremt outsourcingaftalen opsiges.

## 14 Tilsyn med outsourcete funktioner

100. Institutter og betalingsinstitutter bør løbende overvåge tjenesteudbydernes arbejde med hensyn til alle outsourcingordninger ud fra en risikobaseret tilgang og med hovedfokus på outsourcing af kritiske eller vigtige funktioner, herunder at tilgængeligheden, integriteten og sikkerheden af data og oplysninger er sikret. Hvis risikoen, arten eller omfanget af en outsourcet funktion væsentligt har ændret sig, bør institutter og betalingsinstitutter revurdere, om funktionen er kritisk eller vigtig i overensstemmelse med afsnit 4.
101. Institutter og betalingsinstitutter bør anvende passende dygtighed, omhu og hurtighed, når de overvåger og styrer outsourcingordninger.
102. Institutter bør løbende ajourføre deres risikovurdering i henhold til afsnit 12.2 og bør periodisk aflægge rapport til ledelsesorganet om de risici, der er identificeret i forbindelse med outsourcing af kritiske eller vigtige funktioner.
103. Institutter og betalingsinstitutter bør overvåge og styre deres interne koncentrationsrisici som følge af outsourcingordninger under hensyntagen til afsnit 12.2 i disse retningslinjer.
104. Institutter og betalingsinstitutter bør løbende sikre, at outsourcingordninger med hovedfokus på outsourcete kritiske eller vigtige funktioner opfylder de relevante resultat- og kvalitetsstandarder i overensstemmelse med deres politikker ved at:
  - a. sikre, at de modtager passende rapporter fra tjenesteudbydere
  - b. evaluere tjenesteudbydernes resultater ved hjælp af værktøjer såsom KPI'er, centrale kontrolindikatorer, rapporter om udførelsen af tjenesterne, selvcertificering og uafhængige gennemgange og
  - c. gennemgå alle andre relevante oplysninger modtaget fra tjenesteudbyderen, herunder rapporter om forretningskontinuitetsforanstaltninger og -test.
105. Institutter bør træffe passende foranstaltninger, hvis de finder mangler i varetagelsen af den outsourcete funktion. Især bør institutter og betalingsinstitutter følge op på eventuelle tegn på, at tjenesteudbydere ikke kan varetage den outsourcete kritiske eller vigtige funktion effektivt eller i overensstemmelse med gældende love og myndighedskrav. Hvis der konstateres mangler, skal institutter og betalingsinstitutter træffe passende korrigerende og afhjælpende foranstaltninger. Sådanne handlinger kan omfatte opsigelse af outsourcingaftalen, om nødvendigt med øjeblikkelig virkning.

## 15 Exitstrategier

106. Institutter og betalingsinstitutter bør have en dokumenteret exitstrategi, når de outsourcer kritiske eller vigtige funktioner, der er i overensstemmelse med deres outsourcingpolitik og forretningskontinuitetsplaner<sup>37</sup>, som minimum under hensyntagen til muligheden for:
- a. opsigelse af outsourcingordninger
  - b. tjenesteudbyders svigt
  - c. forringelse af kvaliteten af den leverede funktion og faktiske eller potentielle forretningsmæssige afbrydelser forårsaget af uhensigtsmæssig eller manglende varetagelse af funktionen
  - d. Væsentlige risici i forhold til passende og kontinuerlig anvendelse af funktionen.
107. Institutter og betalingsinstitutter bør sikre, at de er i stand til at afslutte outsourcingordninger uden unødigt afbrydelse af deres forretningsaktiviteter, uden at begrænse deres overholdelse af myndighedskrav, og uden det er til skade for kontinuiteten og kvaliteten af dets levering af tjenester til kunder. For at opnå dette bør de:
- a. udvikle og gennemføre exitplaner, som er omfattende, dokumenteret og, hvor det er relevant, tilstrækkeligt testet (f.eks. ved at foretage en analyse af de potentielle omkostninger, konsekvenser, ressourcer og tidsmæssige konsekvenser af at overføre en outsourcet tjeneste til en alternativ tjenesteudbyder) og
  - b. finde alternative løsninger og udvikle overgangsplaner for, at instituttet eller betalingsinstituttet fjerner outsourcete funktioner og data fra tjenesteudbyderen og overfører dem til alternative tjenesteudbydere eller tilbage til instituttet eller betalingsinstituttet, eller træffe andre foranstaltninger, der sikrer kontinuerlig levering af den kritiske eller vigtige funktion eller forretningsaktivitet på en kontrolleret og tilstrækkeligt testet måde, idet der tages hensyn til de udfordringer, der kan opstå på grund af datalokaliteten, og træffe de nødvendige foranstaltninger for at sikre forretningskontinuiteten i overgangsfasen.
108. Ved udvikling af exitstrategier bør institutter og betalingsinstitutter:
- a. definere målene for exitstrategien
  - b. udføre en konsekvensanalyse, der står i rimeligt forhold til risikoen ved de outsourcete processer, tjenester eller aktiviteter, til formålet med at finde frem til, hvilke

---

<sup>37</sup> Institutter i overensstemmelse med kravene i artikel 85, stk. 2, i direktiv 2013/36/EU og del VI i EBA's retningslinjer for intern ledelse og betalingsinstitutter bør have indført passende forretningskontinuitetsplaner med hensyn til outsourcing af afgørende eller væsentlige funktioner.

menneskelige og finansielle ressourcer der vil være påkrævet for at gennemføre exitplanen, og hvor lang tid det vil tage

- c. tildele roller, ansvar og tilstrækkelige ressourcer med henblik på styringen af exitplanerne og overgangsaktiviteterne
- d. definere succeskriterier for overføring af outsourcete funktioner og data og
- e. definere de indikatorer, der skal anvendes til overvågning af outsourcingordningen (som skitseret i afsnit 14), herunder indikatorer baseret på unacceptable serviceniveauer, der bør udløse exitstrategien.

## Del V – Retningslinjer for outsourcing rettet til de kompetente myndigheder

- 109. Ved etablering af passende metoder til overvågning af institutters og betalingsinstitutters overholdelse af betingelserne for den første tilladelse bør de kompetente myndigheder tilstræbe at finde frem til, om outsourcingordninger udgør en væsentlig ændring af betingelser og forpligtelser i institutters og betalingsinstitutters første tilladelse.
- 110. De kompetente myndigheder bør sikre, at de effektivt kan overvåge institutter og betalingsinstitutter, herunder at institutter eller betalingsinstitutter inden for deres outsourcingordning har sikret, at tjenesteudbydere er forpligtet til at give revisions- og adgangsrettigheder til den kompetente myndighed og instituttet i overensstemmelse med afsnit 13.3.
- 111. Analysen af institutternes outsourcingrisici bør som minimum udføres inden for SREP eller, for så vidt angår betalingsinstitutter, som en del af andre tilsynsprocesser, herunder ad hoc-anmodninger, eller under inspektioner på stedet.
- 112. I fortsættelse af de oplysninger, der registreres i registret som nævnt i afsnit 11, kan de kompetente myndigheder anmode institutter og betalingsinstitutter om yderligere oplysninger, navnlig om kritiske eller vigtige outsourcingordninger, såsom:
  - a. en detaljeret risikoanalyse
  - b. hvorvidt tjenesteudbyderen har en forretningskontinuitetsplan, der er hensigtsmæssig for de tjenester, der leveres til det outsourcingende institut eller betalingsinstitut
  - c. den exitstrategi, som skal anvendes, hvis outsourcingordningen opsiges af en af parterne, eller hvis der sker afbrydelser af leveringen af tjenesterne, og
  - d. de ressourcer og foranstaltninger, som er indført til at overvåge de outsourcete aktiviteter på passende vis.

113. Ud over de oplysninger, der kræves i henhold til afsnit 11, kan de kompetente myndigheder kræve, at institutter og betalingsinstitutter skal give detaljerede oplysninger om alle outsourcingordninger, selv om den pågældende funktion ikke anses for kritisk eller vigtig.
114. De kompetente myndigheder bør vurdere følgende ud fra en risikobaseret tilgang:
- om institutter og betalingsinstitutter overvåger og administrerer især kritiske eller vigtige outsourcingordninger hensigtsmæssigt
  - om institutter og betalingsinstitutter har indført tilstrækkelige ressourcer til overvågning og styring af outsourcingordninger
  - om institutter og betalingsinstitutter afdækker og styrer alle relevante risici, og
  - om institutter og betalingsinstitutter afdækker, vurderer og på passende vis styrer interessekonflikter med hensyn til outsourcingordninger, f.eks. i tilfælde af koncernintern outsourcing eller outsourcing i den samme institutsikringsordning.
115. De kompetente myndigheder bør sikre, at EU/EØS-institutter og betalingsinstitutter ikke fungerer som en "tom skal", herunder i situationer, hvor institutter bruger back-to-back-transaktioner eller koncerninterne transaktioner til at overføre en del af markeds- og kreditrisikoen til en ikke-EU/EØS-enhed, og bør sikre, at de har indført de rigtige ledelses- og risikostyringsordninger til at afdække og styre deres risici.
116. I deres vurdering bør de kompetente myndigheder tage hensyn til alle risici, især:<sup>38</sup>
- de operationelle risici<sup>39</sup>, som outsourcingordningen udgør
  - omdømmemæssige risici
  - "step-in"-risikoen, som kan kræve, at instituttet redder en tjenesteudbyder i tilfælde af væsentlige institutter
  - koncentrationsrisici i instituttet, herunder på et konsolideret grundlag, forårsaget af flere outsourcingordninger med en enkelt tjenesteudbyder eller tæt forbundne tjenesteudbydere eller flere outsourcingordninger inden for samme forretningsområde
  - koncentrationsrisici på sektorniveau, f.eks. hvor flere institutter eller betalingsinstitutter gør brug af en enkelt tjenesteudbyder eller en lille gruppe af tjenesteudbydere

---

<sup>38</sup> For institutter, der er underlagt direktiv 2013/36/EU: Se også EBA's retningslinjer for SREP: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

<sup>39</sup> Se også EBA's retningslinjer for IKT-risiko: <https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a>

- f. i hvilket omfang outsourcinginstituttet eller -betalingsinstituttet kontrollerer tjenesteudbyderen eller har mulighed for at påvirke dets handlinger, den reduktion af risici, der kan skyldes en højere grad af kontrol, og om tjenesteudbyderen er omfattet af det konsoliderede tilsyn med koncernen, og
- g. interessekonflikter mellem instituttet og tjenesteudbyderen.

117. Såfremt der afdækkes koncentrationsrisici, bør de kompetente myndigheder overvåge udviklingen af sådanne risici og vurdere både deres potentielle indvirkning på andre institutter og betalingsinstitutter og stabiliteten af det finansielle marked. De kompetente myndigheder bør, hvor det er relevant, informere afviklingsmyndigheden om nye potentielt kritiske funktioner<sup>40</sup>, der er blevet afdækket i løbet af denne vurdering.

118. Hvor der konstateres bekymringer, hvoraf det kan udledes, at et institut eller betalingsinstitut ikke længere har indført solide ledelsesordninger eller ikke opfylder de lovregulerede krav, bør de kompetente myndigheder træffe passende foranstaltninger, som kan omfatte at begrænse eller indskrænke omfanget af de outsourcete funktioner eller kræve udtrædelse af en eller flere outsourcingordninger. Idet der navnlig tages hensyn til instituttets eller betalingsinstituttets behov for at operere kontinuerligt, kan der stilles krav om annullering af kontrakter, hvis tilsyn med og håndhævelse af de lovregulerede skrav ikke kan sikres ved andre foranstaltninger.

119. De kompetente myndigheder bør kontrollere, at de er i stand til at udføre et effektivt tilsyn, især når institutter og betalingsinstitutter outsourcer kritiske eller vigtige funktioner, der er gennemført uden for EU/EØS.

---

<sup>40</sup> Som defineret i artikel 2, stk. 1, nr. 35), i BRRD.