ERHVERVSMINISTERIET

5. januar 2021

GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

Kommissionens forslag til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor (digital operationel robusthed - DORA) (KOM 2020/595)

1. Resumé

Kommissionen offentliggjorde den 24. september 2020 en pakke på området for digital finansiering. Pakken består bl.a. af forslag til forordning om digital operationel robusthed (DORA). Baggrunden for forslaget er et ønske om at imødegå de problemstillinger som den stadigt stigende digitalisering af den finansielle sektor i EU indebærer.

Hensigten med forslaget er overordnet at bidrage til at skabe en mere sikker og effektiv digital finansiel sektor ved at opstille en række harmoniserede EU-krav og regler for finansielle virksomheder.

Forordningens tiltag falder inden for fire områder: 1) krav til finansielle virksomheders ledelse (fx kreditinstitutter), risikostyring, rapportering og cybersikkerhed; 2) krav til udformningen af kontrakter mellem finansielle virksomheder og evt. it-leverandører; 3) rammer for fælles overvågning med kritiske tredjeparts it-leverandører; og 4) rammer for tilsyn, håndhævelse og samarbejde mellem kompetente myndigheder.

Forordningen er ledsaget af et direktiv med ændringer i andre direktiver som følge af forordningen.

Regeringen støtter formålet og ser generelt positivt på forslaget til forordning. Det er vigtigt for regeringen at sikre en effektiv og digitalt fremtidssikret finansiel sektor, som kan fortsætte med at levere de løsninger, som forbrugere og virksomheder efterspørger.

Forslaget skal bidrage til at sikre den finansielle stabilitet, og regeringen lægger i den forbindelse vægt på, at betalingsinfrastrukturer bliver omfattet

af anvendelsesområdet, henset til deres væsentlige samfundsmæssige funktion. Regeringen vil desuden arbejde for, at reglerne for de mindre finansielle aktører på området bliver mere proportionale ift. deres risici.

2. Baggrund

Den digitale transformation af den finansielle sektor har medført en række udfordringer, som bl.a. består af en forøget teknisk afhængighed og koncentration på færre – og større – leverandører, som i væsentligt omfang falder uden for den eksisterende europæiske finansielle regulering og tilsyn. Dertil kommer et generelt stigende niveau for cyberrisici i den finansielle sektor.

En særlig gruppe af leverandører, som den finansielle sektor gør øget brug af, er leverandørerne af cloudtjenester[1], som har vundet væsentlige markedsandele i alle dele af den finansielle sektor i EU, på grund af disse tjenesters fleksibilitet og skalérbarhed. Cloudleverandørernes størrelse, forretningsmodeller og kontraktstyper har medført en række udfordringer i forhold til reguleringen af de finansielle virksomheders it-risikostyring.

Fremkomst af store leverandører, herunder særligt cloudleverandører, indebærer, at store dele af it-drift og en væsentlig del af it-udviklingen i dag bliver varetaget af selskaber, som de finansielle virksomheder ikke har kontrol med og indblik i – og som typisk kun giver de finansielle virksomheder valget mellem standardprodukter. Det stiller væsentligt højere krav til styringen af kontrakterne med leverandørerne, og omvendt færre krav til styring af konkret it-drift.

Det forhold, at ingen af cloudleverandørerne aktuelt er hjemmehørende inden for EU er problematisk i tilsynsøjemed og stiller derfor yderligere krav til virksomhedernes håndhævelse af kontrakterne og de kompetente myndigheders håndhævelse af den finansielle lovgivning, der generelt stiller krav til finansielle virksomheders it-sikkerhed. Cloudleverandørernes grænseoverskridende karakter og det, at reglerne om tilsyn ikke kan håndhæves direkte over for virksomheder uden for EU, har skabt et behov for en mere fundamental revision af reglerne om it-tilsyn, end hvad der hidtil har været tilfældet.

En styrkelse af den finansielle sektors digitale sikkerhed indgik allrede i Kommissionens fintech handlingsplan fra marts 2018[2], og de tre europæiske tilsynsmyndigheder Den Europæiske Banktilsynsmyndighed (EBA),

[1] Cloudtjenester er services som udbydes via internettet af en leverandør og som regel ikke kræver fx intern infrastruktur eller hardware hos den købende part. De største leverandører i dag af cloudtjenester er bl.a. Microsoft, Amazon, Google, Apple og Alibaba.
[2] KOM/2018/0109 final

Den Europæiske Værdipapir- og Markedsmyndighed (ESMA) og Den Europæiske Pensions- og Forsikringsmyndighed (EIOPA) – under samlebetegnelsen "ESA'erne", udarbejdede i april 2019 et såkaldt "Joint Advice"[3] til Kommissionen, der identificerede en række områder med behov for lovgivningsmæssige forbedringer.

Hjemlen til den foreslåede forordning og direktiv er TFEU art. 114, og både forordningen og direktivet skal vedtages af både Rådet og Parlamentet.

3. Formål og indhold

Formålet med forslaget om digital operationel robusthed (Digital Operational Resilience Act, DORA) er at modernisere og harmonisere de regler, der gælder for digitale operationelle risici, dvs. finansielle virksomheders it-risici som følge af forandringerne i teknologianvendelsen i den finansielle sektor. Harmoniseringen og moderniseringen ventes at gøre efterlevelsen af reglerne nemmere i lyset af de forhindringer og den fragmentering, som anvendelsen af de nuværende regler indebærer i forhold til de finansielle virksomheders anvendelse af nye digitale muligheder.

Et væsentligt princip, som Kommissionen følger i dette arbejde, er princippet om "samme risici, samme regler, samme regulering", som grundlæggende handler om at sikre lige konkurrencevilkår og tilstrækkelig sikkerhed.

For at sikre en sammenhæng til de krav der stilles med forordningen omfatter forordningen størstedelen af den finansielle sektor samt revisorer og revisionsfirmaer. Den brede dækning har til hensigt at fremme en homogen og sammenhængende anvendelse af alle de komponenter, der indgår i en risikostyring.

Kommissionens forslag bygger i al væsentlighed på anbefalingerne i ESA'ernes Joint Advice med et fælles overordnet regelsæt, som med kun enkelte undtagelser, bl.a. betalingsinfrastrukturer[4], gælder for hele den fi-

[3] JC 2019 26

[4] Med »betalingsinfrastrukturer« menes i denne sammenhæng operatører af detailbetalingssystemer, dvs. systemer til clearing (sumclearing, intradag clearing og straksclearing) af almindelige betalinger mellem forbrugere, virksomheder og offentlige myndigheder mv.

nansielle sektor, dvs. på kredit- og betalingsområdet, forsikrings- og pensionsområdet og på kapitalmarkedsområdet[5], og med delegation til at gennemføre mere sektorspecifikke delegerede retsakter og gennemførselsbestemmelser.

Forslaget består af en forordning med en række detaljerede regler og et ændringsdirektiv, som har til formål at gennemføre ændringer i allerede eksisterende direktiver på det finansielle område ved at indsætte henvisninger til DORA-forordningen i relevante EU-retsakter.

Forordningen indeholder regler på fire områder:

1) Krav til finansielle virksomheders ledelse, risikostyring, rapportering og cybersikkerhed
2) Krav til udformning af kontrakter mellem finansielle virksomheder og evt. it-leverandører
3) Rammer for fælles overvågning af kritiske tredjeparts it-leverandører
4) Rammer for tilsyn, håndhævelse og samarbejde mellem kompetente myndigheder

3.1 Krav til finansielle virksomheders ledelse, risikostyring, rapportering og cybersikkerhed

Kommissionens forslag indeholder bl.a. en række krav til de finansielle virksomheders ledelse og risikostyring. Generelt for kravene er, at de har til formål at sikre en konsistent og ensartet håndtering af cyberrisici i de finansielle virksomheder, således at trusler mv. håndteres korrekt både før, under og efter hændelsen. Kravene går bl.a. på retningslinjer for håndteringen af trusler, offentliggørelsesplan mv. For risikostyringsdelen vedrører kravene dialog med de kompetente myndigheder om håndteringen af risici, løbende risikovurdering/monitorering, opfølgning og afrapportering til ledelsen mv.

[5] Forslaget omfatter specifikt følgende virksomhedstyper: kreditinstitutter, betalingsinstitutter, e-pengeinstitutter, investeringsselskaber, kryptoaktivtjenester, udstedere af kryptoaktiver, udstedere af aktivbaserede tokens samt udstedere af signifikante aktivbaserede tokens, værdipapircentraler, centrale modparter, regulerede markeder, transaktionsregistre, forvaltere af alternative investeringsfonde, investeringsforvaltningsselskaber, udbydere af dataindberetningstjenester, forsikrings- og genforsikringsvirksomheder, forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, arbejdsmarkedspensionsselskaber, kreditvurderingsbureauer, godkendte revisorer og revisionsselskaber, administratorer af kritiske benchmarks, crowdfundingtjenesteudbydere, securitisation repositories, og it-leverandører.

Der foreslås også krav om hændelsesrapportering, der bl.a. handler om oprettelse af processer for detektering samt håndtering af og notificering om it-hændelser.

Vedrørende testning stilles der krav om løbende tests af it-sikkerheden, såkaldte trusselsbaserede penetrationstests (threat led penetration tests (TLPT)), som de kompetente myndigheder kan pålægge finansielle virksomheder at gennemføre under hensyntagen til bl.a. virksomhedernes størrelse.

Forslaget om god risikostyring af tredjepartsrisici indeholder forslag, der bl.a. indebærer, at de finansielle virksomheder skal træffe passende foranstaltninger baseret på afhængighedsgraden af tredjeparter. Herudover er der bl.a. krav om jævnlig rapportering til de kompetente myndigheder om brugen af tredjeparts it-leverandører, herunder hvornår kritiske funktioner er involveret. Virksomhederne skal også udarbejde en strategi for håndtering af risici forbundet med virksomhedens brug af tredjeparts it-leverandører. Der stilles også krav til omgående annullering af kontrakter såfremt disse ikke overholdes af tredjeparterne.

Der er i forslaget indlagt mulighed for proportionalitet, og meget små virksomheder (de såkaldte mikrovirksomheder[6]) er helt undtaget fra nogle af kravene, herunder bl.a. krav om særlige roller og særlige systemer til it-sikkerhedsstyring.

3.2 krav til udformning af kontrakter mellem finansielle virksomheder og evt. it-leverandører

Kommissionens forslag til kontraktkrav indeholder bl.a. en række governancekrav og nogle generelle minimumskrav til elementer i kontrakterne med væsentlige leverandører, ligesom der kan være specifikke elementer afhængig af den ydelse kontrakten angår. Det kan og vil ofte være en fordel for finansielle virksomheder, at der er minimumskrav til indholdet i kontrakter, da store it-leverandører på grund af det asymmetriske styrkeforhold ellers kan gennemtvinge kontrakter med mere diffuse krav, ligesom at kontrakterne giver de finansielle virksomheder sikkerhed for, hvilken service det er, at it-leverandørerne skal levere og hvordan.

Kravene omfatter bl.a. oplysning om alle funktioner og services som tredjeparten skal levere, herunder videreoutsourcing af disse, oplysning om hvor databehandling finder sted, oplysning fra tredjepart til den finansielle virksomhed om substantielle ændringer hos tredjepart, som kan have konsekvenser for de tilkøbte services, krav om specifikke sikkerhedsforanstaltninger hos tredjepart, krav om beredskabsplaner hos leverandøren, krav om forpligtelse af leverandøren til at samarbejde med tilsynsmyndigheder,

[6] Virksomheder med under 10 ansatte og en omsætning på mindre end 10 mio. euro.

krav om den finansielle virksomheds ret til at overvåge leverandørens opgaveløsning og krav til leverandørens samarbejde om kundens ophør af leverandørforholdet.

Kravene skal styrke de finansielle virksomheders muligheder for at styre de risici, der er forbundet med afhængigheder af tredjeparter.

3.3 Rammer for fælles overvågning af kritiske tredjeparts it-leverandører

Kommissionens forslag indebærer opsætning af et fælles tilsynsregime med såkaldte kritiske tredjeparts it-leverandører[7] og et system for udpegning af kritiske tredjeparts it-leverandører.

Det Fælles Udvalg af Europæiske Tilsynsmyndigheder[8] nedsætter et *overvågningsforum (oversight forum)* som et underudvalg bestående af ESA'ernes formænd og repræsentanter fra de nationale kompetente myndigheder.

Dette forum skal bidrage til Det Fælles Udvalgs udpegning af kritiske leverandører og udpegning af en *ansvarlig tilsynsmyndighed (Lead Overseer)*, som skal være en af de tre ESA'er (ESMA, EBA eller EIOPA), afhængigt af specifikke kriterier hos leverandøren.

Der vil blive oprettet tilsynskollegier til formålet, som de ansvarlige tilsynsmyndigheder sammensætter med repræsentanter fra højst 10 af de i forhold til leverandøren relevante medlemsstater til at gennemføre løbende tilsyn med leverandørerne.

Udpegningen af kritiske tredjeparts it-leverandører er i Kommissionens forslag baseret på en række forskellige grænseværdier, herunder fx den systemiske konsekvens i tilfælde af et større nedbrud hos leverandøren, mængden og afhængigheden heraf for finansielle institutioner, som benytter sig af leverandøren, graden af alternative leverandører på markedet af en given service, antallet af EU-medlemslande i hvilke it-leverandørens services bruges mv. Der skal årligt publiceres en liste over kritiske it-leverandører.

Med forslaget lægges der op til at forbyde brugen af kritiske it-leverandører, som ikke er etableret i EU – et såkaldt lokaliseringskrav. Ligeledes vil det fælles tilsynsregime kun skulle føre direkte tilsyn med kritiske tredjeparts it-leverandører, som er etableret i EU.

---

[7] Det er ikke oplyst, hvilke it-leverandører der vil blive klassificerede som kritiske, men forventningen fra Kommissions side er dog, at ca. 10-15 virksomheder vil være omfattede. Eksempler på mulige kandidater er bl.a. Bloomberg, Amazon Web Services, Refinitiv, Google, Microsoft, Alibaba, Huawei, Apple og Cisco.

[8] Jf. forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Det fælles tilsynsregime indebærer overvågning af kritiske tredjepartsleverandører, herunder vurdering af it-leverandørens risikostyring, ledelse, fysiske sikkerhedsforanstaltninger mv. Den relevante tilsynsmyndighed vil bl.a. have ret til alle relevante data, udførelse af inspektioner, herunder også on-site, udstedelse af bødeforlæg mv.

Der gives ikke mulighed for at udstede påbud om – eller forbud mod bestemte aktiviteter hos de kritiske leverandører, men der er hjemmel til bøder mv. såfremt leverandørerne ikke samarbejder om tilsyn og dokumentation.

Der stilles også krav til procedureregler for samarbejdet mellem de nationale kompetente myndigheder angående bl.a. årlige vurderinger af tilsynsfunktionen og drøftelser af udviklingen på området. De kritiske it-leverandører vil blive pålagt gebyrer mhp. at dække omkostninger ved driften af tilsynet.

Opfølgningen på inspektionsrapporterne fra de europæiske tilsynsmyndigheder sker mellem de nationale tilsynsmyndigheder og de finansielle virksomheder, der anvender de pågældende leverandører.

3.4 Rammer for tilsyn, håndhævelse og samarbejde mellem kompetente myndigheder

Kommissionens foreslår at oprette en fælles rapporteringsfunktion, hvortil rapportering af større it-hændelser kan ske for dermed bl.a. at sikre et tæt samarbejde med det fælles tilsyn og give nationale kompetente myndigheder mulighed for at udveksle viden, erfaringer mv. på området med hinanden. Samarbejdet skal bl.a. bidrage til udviklingen af en koordineret tilgang og respons ved større it-nedbrud.

4. Europa-Parlamentets udtalelse

Europa-Parlamentet har endnu ikke udtalt sig om forslaget. Europa-Parlamentet er sammen med Rådet, medlovgiver på forslaget. Europa-Parlamentet har tidligere opfordret Kommissionen til at fremsætte lovforslag på området for cybermodstandsdygtighed, herunder fsva. tilsyn med kritiske tredjepartsleverandører samt modernisering og harmonisering af de nuværende regler på området[9].

5. Nærhedsprincippet

Kommissionen angiver, at den grænseoverskridende karakter og udbredte afhængighed af tredjepartsleverandørers digitale tjenester i den finansielle sektor koblet med manglen på harmoniseret regulering kun kan håndteres effektivt på EU-niveau.

[9] www.europarl.europa.eu/doceo/document/TA-9-2020-0265_DA.html

Regeringen er enig i Kommissionens vurdering af, at regulering og tiltag i de enkelte EU-lande ikke er tilstrækkeligt til at adressere de grænseoverskridende udfordringer, og det er på den baggrund regeringens vurdering, at forslaget er i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret

Regelsættet for forpligtelser til it-risikostyring og betryggende kontrol- og sikringsforanstaltninger på it-området er meget forskellig i både indhold og detaljeringsgrad på de forskellige område inden for den finansielle sektor.

Med undtagelse af reglerne for tilsyn med fælles datacentraler har de forskellige regler hjemmel i de relevante EU-retsakter, og den nationale implementering af disse, hvor der er tale om direktiver.

Reglerne er bl.a. implementeret i lov om finansiel virksomhed, betalingsloven, kapitalmarkedsloven og en række andre love på mere specifikke områder samt bekendtgørelser udstedt i henhold til disse. På flere områder har Kommissionen udstedt delegerede retsakter, som gælder direkte, eller henstillinger og vejledninger, hvoraf flere er implementeret ved bekendtgørelser eller som udgør fortolkningsgrundlag i forhold til mere generelle danske regler. Visse bekendtgørelser gælder for flere områder, herunder outsourcingbekendtgørelserne[10][11] og bilag 5 i bekendtgørelse om ledelse og styring af pengeinstitutter[12].

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Den nationale lovgivning skal i relevant omfang ændres eller ophæves, da forordningen, ændringsdirektivet og de kommende delegerede retsakter vil træde i stedet for.

Økonomiske konsekvenser

Statsfinansielle konsekvenser

Forslaget ventes ikke at have statsfinansielle konsekvenser.

Med forordningen indføres nye krav til tilsyn, som også vil omfatte virksomhedstyper, som ikke i dag er under tilsyn. På samme vis vil deltagelsen i et evt. fælles tilsyn under ESA'erne også været forbundet med en række administrative omkostninger og øget ressourceforbrug.

[10] BEK nr. 877 af 12/06/2020
[11] BEK nr. 723 af 28/05/2020
[12] BEK nr. 1026 af 30/06/2016

I Danmark finansieres omkostninger ved tilsyn af de finansielle virksomheder under tilsyn. ESA'erne er finansieret delvist nationalt af EU-landene og delvist via EU-budgettet.

Samfundsøkonomiske konsekvenser
Forslaget forventes at have positive samfundsøkonomiske konsekvenser, dels ved at styrke cyberrobustheden i den finansielle sektor, dels ved at sikre større klarhed og harmonisering i regelsættet på området på tværs af EU-landene.

Harmoniseringen af reglerne sikrer herudover mod regulatorisk arbitrage i forhold til andre EU-lande, der i dag måtte have lempeligere regler på området end Danmark.

Erhvervsøkonomiske konsekvenser
For visse af de berørte virksomhedstyper i Danmark afspejler reglerne i Kommissionens forslag i vidt omfang de krav, virksomhederne allerede er underlagt i dag. Det er hovedsageligt virksomheder uden for områderne for banker, betalingsinstitutter, finansielle infrastrukturer og datacentraler, som vil skulle leve op til nye eller skærpede krav.

De nye regler kan få betydning for måden hvorpå de finansielle virksomheder organiserer deres it-styring, foretager risikostyring, indgår outsourcingkontrakter, rapporterer hændelser og tester systemer. Langt størstedelen af de indholdsmæssige krav til dette stilles imidlertid allerede i dag i Danmark, men får med forordningen et mere tydeligt og ensartet ophæng.

Overvågning af tredjepartsleverandører, som er kritiske på europæisk niveau, vil potentielt kunne lette både de finansielle virksomheder og deres fælles datacentraler for en del af byrden ved at skulle redegøre for disse leverandørers risikostyring mv. Den del af forslaget ventes derfor ikke at få væsentlige negative erhvervsøkonomiske konsekvenser.

Andre konsekvenser og beskyttelsesniveau
Forslaget forventes ikke at have konsekvenser for beskæftigelsen, arbejdsmarkedet, ligestilling, miljø eller sundhed i Danmark.

8. Høring

Forslaget har været sendt i høring i EU-specialudvalget for den finansielle sektor med svarfrist den 8. oktober 2020. Der er modtaget høringssvar fra Finans Danmark (FIDA) og Forsikring & Pension (F&P). Nedenfor sammenfattes indholdet af de to indkomne høringssvar.

FIDA og F&P byder begge Kommissionens forslag velkommen.

FIDA udtrykker stor opbakning til indholdet i forslaget og finder det positivt, at der lægges op til en harmonisering af reglerne i den finansielle sektor på området. FIDA ønsker blandt andet, at reglerne skal være risikobaserede, sammenhængende og være med til at sikre en bedre koordinering mellem EU-landene. FIDA har dog også nogle bekymringer ift. proportionaliteten i forslaget, hvor FIDA opfordrer til større klarhed i regelsættet, ligesom mindre aktører på det finansielle område ikke bør rammes unødvendigt. FIDA udtrykker også støtte til et fælles EU-tilsyn med kritiske tredjepartsleverandører.

F&P udtrykker generelt opbakning til forslaget og finder det positivt, at der er lagt op til harmonisering og ensretning af reglerne på området. F&P efterlyser dog, at der i forslaget tages bestik af den anderledes risikoprofil, som forsikrings- og pensionsselskaber har vis-a-vis banksektoren. F&P er ligeledes bekymret for implementeringshastigheden pga. de generelt omfattende og komplekse krav i forslaget, som kræver både investeringer og tilstrækkelig tid at få på plads. Endelig ønsker F&P større klarhed, særligt på området for tilsyn med kritiske tredjepartsleverandører.

9. Generelle forventninger til andre landes holdninger

Forslaget har generelt fået en positiv modtagelse blandt EU-landene.

Der har dog – fra forskellige grupperinger af EU-lande – været udtrykt behov for større klarhed i teksten, herunder særligt i forhold til sammenhæng og præcedens med anden eksisterende sektorspecifik lovgivning på området. Derudover har flere lande ytret ønske om inklusion af betalingsinfrastrukturer i forslagets anvendelsesområde. Endvidere mener flere medlemslande, at revisorer skal delvist undtages fra forslaget, og at forslaget bør indeholde mere proportionalitet for mindre finansielle virksomheder.

Muligheden for et fælles tilsyn med kritiske it-leverandører har modtaget umiddelbar opbakning blandt medlemslandene om end beføjelserne, strukturen og kriterierne er genstand for drøftelser.

10. Regeringens foreløbige generelle holdning

Cyberrisici mod den finansielle sektor er høje, og usikkerheder og risici hos mindre finansielle virksomheder kan skabe sårbarheder hos de mindre, men også de større finansielle virksomheder.

Regeringen støtter overordnet forslagets formål om at sikre en mere effektiv og sikker digital finansiel sektor via en række harmoniserede krav og regler. Samlet set vurderes forslaget at styrke cyberrobustheden i Danmark.

It-risici får en stadigt større betydning for driften i de finansielle virksomheder, og regeringen finder det derfor væsentligt, at lovgivningen følger

med udviklingen i it-anvendelsen i sektoren, og at overlap i gældende regler på tværs af den finansielle sektor minimeres. Et andet element er at sikre ensartede regler og samarbejde på tværs af alle EU-landene, da it-risici er grænseoverskridende, herunder vedrører tredjelande.

Regeringen støtter, at der kommer mere ensartede og tydeligere regler om ledelse og risikostyring på it-området.

Regeringen lægger vægt på, at betalingsinfrastrukturer bør omfattes af forordningens anvendelsesområde. Clearing og afvikling af betalinger er blevet en væsentlig samfundsmæssig funktion i takt med, at næsten alle almindelige danske betalinger sker digitalt. Et cyberangreb mod betalingsinfrastrukturen kan dermed have væsentlige systemiske konsekvenser, hvorfor regeringen finder, at der er behov for også at underlægge disse virksomhedstyper krav i forhold til operationelle risici.

Regeringen arbejder for, at revisorer og revisionsvirksomheder delvist bør undtages fra forslaget. Forslaget omfatter for nuværende alle revisorer og revisionsvirksomheder, uanset om de pågældende har finansielle virksomheder som revisionskunder, hvilket ikke forekommer proportionalt under hensyn til sigtet med forordningen. En eventuel inklusion af revisionsvirksomheder i forordningen bør begrænses til revisionsvirksomheder, som har finansielle virksomheder som revisionskunder.

Regeringen vil arbejde for, at forslaget indeholder klarere og mere fremtidssikrede regler om styring af tredjepartsrisici i sammenligning med de nuværende regler om outsourcing.

Regeringen er åben over for et fælleseuropæisk tilsyn med væsentlige tredjepartsudbydere, og lægger vægt på, at de nationale tilsynsmyndigheders erfaringer og viden om nationale forhold og markeder inddrages. Det er vigtigt med et stærkt og omkostningseffektivt tilsyn med infrastruktur, der drives af tredjepartsleverandører. Et fælles tilsyn ventes bedre at kunne modvirke at tredjepartsudbyderne kan omgå tilsyn ved at placere sig i lande med mindre restriktive tilgange. Der skal etableres et stærkt og effektivt tilsyn, som bør være samlet hos én europæisk tilsynsmyndighed, der tildeles kompetencer, hvor der er et klart rationale herfor, og alene tildeles direkte tilsynskompetencer på de områder, hvor der er tale om væsentlig grænseoverskridende aktiviteter, og hvor området ikke vurderes at kunne håndteres lige så godt eller bedre på nationalt plan.

I den sammenhæng er det vigtigt at understrege, at et fælles europæisk tilsyn ikke må rykke ved ansvarsfordelingen. Det skal fortsat være de finansielle virksomheder, der er forpligtet til at styre risiciene ved outsourcing til tredjepartsudbydere.

Regeringen er åben over for at se nærmere på om et lokaliseringskrav eller lignende er hensigtsmæssige tiltag til at løfte denne opgave.

Regeringen finder, at der bør tages større hensyn til proportionalitet i forslaget. Regeringen finder det positivt, at ikke kun mikrovirksomheder skal kunne opnå undtagelser fra visse krav til ledelse mv., men at der bør kigges bredere, således at andre mindre virksomheder også kan undtages fra visse krav med en begrænset merværdi.

Regeringen vil endvidere arbejde for, at centrale emner håndteres af lovgiverne i forbindelse med udformningen af forordningen og ikke uddelegeres til fx delegerede retsakter, samt at eventuelle bemyndigelser til delegerede retsakter er tilstrækkeligt afgrænsede og indrammede.

Regeringen vil endelig arbejde for, at sektoren har tilstrækkelig tid til omstillingen til det nye regelsæt.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Forslaget har tidligere været forelagt Folketingets Europaudvalg i forbindelse med ECOFIN den 6. oktober 2020, hvor udvalget modtog et samlenotat herom.