U 58/2020 rd

Statsrådets skrivelse till riksdagen om kommissionens förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft i den finansiella sektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014 och till direktiv om ändring av direktiven 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 och EU/2016/2341 (*Digital operativ motståndskraft i den finansiella sektorn*)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen kommissionens förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft i den finansiella sektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, kommissionens förslag till Europaparlamentets och rådets direktiv om ändring av direktiven 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 och EU/2016/2341, samt en promemoria om förslagen.

Helsingfors den 5 november 2020

Finansminister Matti Vanhanen

Regeringssekreterare Jonna Kuparinen

FINANSMINISTERIET PROMEMORIA EU/2020/1428
EU/2020/1436
19.10.2020

FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM DIGITAL OPERATIV MOTSTÅNDSKRAFT I DEN FINANSIELLA SEKTORN OCH OM ÄNDRING AV FÖRORDNINGARNA (EG) NR 1060/2009, (EU) NR 648/2012, (EU) NR 600/2014 OCH (EU) NR 909/2014 OCH TILL DIREKTIV OM ÄNDRING AV DIREKTIVEN 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 OCH EU/2016/2341

1 Allmänt

Den 24 september 2020 lade kommissionen fram ett förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft i den finansiella sektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, (COM(2020) 595 final), nedan *förslaget till förordning*, och ett förslag till Europaparlamentets och rådets direktiv om ändring av direktiven 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 och EU/2016/2341, (COM(2020) 596 final), nedan *förslaget till direktiv*.

Förslaget till förordning och förslaget till direktiv har överlämnats till Europaparlamentet och rådet för behandling i enlighet med det ordinarie lagstiftningsförfarandet och för antagande inom ramen för medbeslutandeförfarandet. Behandlingen av förslagen i rådet inleddes i september 2020.

Den föreslagna förordningen avses träda i kraft den 20:e dagen efter att den publicerats i Europeiska unionens officiella tidning, och ska börja tillämpas tolv månader efter att den trätt i kraft. Förslaget till direktiv avses träda i kraft den 20:e dagen efter att den publicerats i Europeiska unionens officiella tidning, och ska börja tillämpas tolv månader efter att det trätt i kraft.

2 Förslagens syfte och bakgrund

Förslagen ingår i Strategin för digital finansiering[1], som offentliggjordes av kommissionen den 24 september 2020. Strategin möjliggör och stöder innovations- och konkurrenspotential till digital finansiering och minskar samtidigt de risker som potentialen medför. Ett av kommissionens strategiska mål är att stödja digital finansiering till förmån för konsumenter och företag. Enligt kommissionen ska Europa och den europeiska finansiella sektorn tillägna sig dessa trender och alla möjligheter som den digitala revolutionen erbjuder.

Förslagen till lagstiftning om digital operativ motståndskraft i den finansiella sektorn har sin rot i kommissionens handlingsplan för fintech — ett viktigt steg mot en mer konkurrenskraftig europeisk finanssektor 2018[2]. I enlighet med riktlinjerna för handlingsplanen kartlade de euro-

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Digital Finance Strategy for the EU. (COM(2020) 591 final).
[2] MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA CENTRALBANKEN, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT

peiska finansmarknadsmyndigheterna IKT-säkerheten och styrningen i den europeiska finansiella sektorn och publicerade en gemensam rapport om sina upptäckter den 10 april 2019[3]. Rapporten innehöll rekommendationer för både lagstiftningsändringar efter sektor och sektoröverskridande lagstiftningsändringar. Bland de europeiska finansmarknadsmyndigheterna offentliggjorde Europeiska bankmyndigheten (EBA) och Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) dessutom egna riktlinjer till aktörer om hantering av IKT-risker och säkerhetsrisker i handlingsplanen. I början av 2020 ordnade kommissionen ett offentligt samråd, där kommissionen kartlade olika aktörers syner på hur lagstiftningsramen för digital operativ motståndskraft i den finansiella sektorn skulle kunna genomföras. Även Finland besvarade frågorna.

Digitalisering medför möjligheter och risker vars karaktär ska också förstås ur den finansiella sektorns synvinkel. Den reform av lagstiftningen som följde på finanskrisen 2008 förbättrade i första hand motståndskraften i den europeiska finansiella sektorn, men inte i någon större mån den kapacitet som överskrider den finansiella sektorns gränser. Det faktum att detaljerade och övergripande regler för digital operativ motståndskraft saknats på EU-nivå har lett till nationella initiativ till regelverk, såsom nya tester av motståndskraft och ett ökat antal tillsynsmetoder. Trots att de nationella regleringsprojekten har haft goda mål, har de nationella projekt som inte samordnats på EU-nivå, för aktörernas del, dels lett till överlappande krav, inkonsekvenser och höga administrativa kostnader, framför allt för gränsöverskridande aktörer. Syftet med förslagen är att effektivisera och strömlinjeforma finansmarknadsaktörernas IKT-riskhantering och systemtestning och att öka tillsynsmyndigheternas medvetenhet om cyberrisker som drabbar tillsynsobjekt och om farliga situationer som har samband med IKT-frågor. Dessutom är syftet att ingripa i risker som inte har beaktats på grund av avsaknaden av gemensamma regler.

Förslagen har även samband med de övriga förslagen till rättsakt och handlingsplanerna i Strategin för digital finansiering. I anslutning till strategin offentliggjordes bland annat förslag till förordning om kryptotillgångar[4], nedan *förslagen till förordning om kryptotillgångar*, och en EU-strategi för massbetalningar. På grund av förordnings- och direktivförslagens övergripande karaktär har de även samband med vissa andra EU-rättsakter, såsom nätverks- och informationssystemdirektivet[5] och direktivet om europeisk kritisk infrastruktur[6], vilka för tillfället är föremål för översyn. Förslagen är också förenliga med Europeiska säkerhetsstrategin och handlingsplanen för en kapitalmarknadsunion.

Förslagen kan även anses ha samband med covid-19-pandemin. Enligt kommissionens beräkningar har cyberattackerna mot organisationer ökat med 38 procent under pandemin. Enligt kommissionen bör Europa utnyttja både digitala tjänster och teknik vid tillhandahållande av

---

REGIONKOMMITTÉN Handlingsplanen för fintech – ett viktigt steg mot en mer konkurrenskraftig europeisk finanssektor. (COM/2018/0109 final).

[3] Joint Advice of the European Supervisory Authorities: To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector.

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology. COM/2020/594 final.

[5] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

[6] RÅDETS DIREKTIV 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna.

tjänster så att det främjar tillgången till finansiering och avhjälper de sociala och ekonomiska skador som har orsakats av pandemin. Kommissionen anser att digitalisering spelar en nyckelroll i åtgärderna för att stimulera och modernisera Europas ekonomi mot ett tillväxtspår inom alla sektorer. Syftet med de förslag som behandlas i denna skrivelse är även att främja de uppställda målen.

3 Huvudsakligt innehåll

3.1 Förslag till förordning om digital operativ motståndskraft i den finansiella sektorn

3.1.1 Syfte och tillämpningsområde för förslaget till förordning (artiklarna 1—3)

I förordningen fastställs de gemensamma kraven på säkerhet i IKT-system som stöder finansmarknadsaktörernas affärsprocesser, säkerhet som är nödvändig för att en gemensam digital operativ kapacitet ska kunna nås. De gemensamma kraven gäller IKT-riskhantering, anmälan om betydande IKT-relaterade incidenter till behöriga myndigheter, testning av digital operativ kapacitet, delning av information och underrättelseinformation om näthot och sårbarheter samt åtgärder och hantering av IKT-risker i förhållande till kritiska tredje parter.

I enlighet med kommissionens mål bör förordningen tillämpas på unionens finansiella marknad nästan i sin helhet. Tillämpningsområdet för förslaget till förordning kommer på så sätt att vara brett och omfatta nästan alla aktörer som regleras genom EU:s finansmarknadslagstiftning. Sådana aktörer är åtminstone kreditinstitut, betalningsinstitut, institut för elektroniska pengar, värdepappersföretag, sådana leverantörer och utgivare av virtuell valuta som avses i förslagen till förordning om kryptotillgångar, värdepapperscentraler, förvaringsinstitut, centrala motparter, handelsplatser eller reglerade marknader, multilaterala handelsplattformar och organiserade handelsplattformar, transaktionsregister, förvaltare av alternativa investeringsfonder, fondbolag till investeringsfonder, leverantörer av rapporteringstjänster, försäkrings- och återförsäkringsföretag, försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet, tjänstepensionsinstitut, kreditvärderingsinstitut, lagstadgade revisorer och revisorssammanslutningar, administratörer av referensvärden, sådana leverantörer av gräsrotsfinansieringstjänster som avses i unionens förordning om gräsrotsfinansiering[7] och värdepapperiseringsregister. Tillämpningsområdet för förslaget ska dock inte omfatta bland annat betalningssystem.

Utöver ovannämnda aktörer ska förslaget gälla sådana kritiska tredje parter utanför den finansiella sektorn som tillhandahåller finansmarknadsaktörer IKT-service. Förordningen ska ställa upp minimikrav på avtalsarrangemangen mellan tredje parter och finansmarknadsaktörer. Dessutom ska förordningen fastställa en tillsynsram för externa tjänsteleverantörer och regler för behöriga myndigheter.

Förslaget till förordning ska tillämpas med iakttagande av proportionalitetsprincipen. Det innebär att de skyldigheter som i förordningen fastställs för finansmarknadsaktörer kommer att stå i proportion till organisationens storlek och andra omständigheter. Till följd av proportionalitetsprincipen är till exempel kraven på mikroföretag mindre strikta. Mikroföretag ska definieras

[7] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2020/1503 av den 7 oktober 2020 om europeiska leverantörer av gräsrotsfinansieringstjänster för företag och om ändring av förordning (EU) 2017/1129 och direktiv (EU) 2019/1937.

på samma sätt som i kommissionens rekommendation 2003/361[8], ”företag som sysselsätter färre än 10 personer och vars omsättning eller balansomslutning inte överstiger 2 miljoner euro per år”. På motsvarande sätt ska en så kallad omfattande TLPT-testning (*Threat Led Penetration Testing*) endast tillämpas på finansmarknadsaktörer som har kategoriserats som betydande. Proportionalitetsprincipen ska även avspeglas i rapporteringen av utfallet av riskhändelser, när rapporteringsskyldigheten endast omfattar betydande händelser.

3.1.2 IKT-riskhantering (artiklarna 4—14)

Förslaget till förordning innefattar bestämmelser om IKT-riskhantering. Bestämmelserna ska delas in i bestämmelser om intern styrning i finansmarknadsaktörer och bestämmelser om en ram för riskhantering. För det första ska en organisations ledning bära allmänt ansvar för IKT-riskhanteringen. Ledningen ska själv ansvara för skapandet av en ram för IKT-riskhantering och utvecklingen av ramen. Dessutom ska ledningen bland annat sörja för kontinuitets- och återställningsplanerna för verksamheten, fastställandet av roller och risknivåer för organisationens interna IKT-funktioner, IKT-investeringarna och ordnandet av behövlig utbildning.

Vad gäller själva IKT-riskhanteringsramen ska organisationen kunna ta fram tillräckliga strategier, policyer, protokoll och verktyg för att identifiera, upptäcka och förebygga risker och för att skydda sig mot risker. Organisationen ska även kunna åtgärda IKT-relaterade skadehändelser, återhämta sig efter händelserna och lära sig av händelserna. Utifrån detta ska organisationen även kunna utveckla sina processer och ge sina intressenter information.

Ramen ska ses över varje år och vid behov i anslutning till vissa IKT-relaterade incidenter. Dessutom ska ramen granskas med jämna mellanrum antingen av ett internt organ eller av ett externt organ. Flera frågor som gäller riskhantering har teknisk karaktär och därför ska de europeiska finansmarknadsmyndigheterna definiera dem i form av tekniska tillsynsstandarder.

3.1.3 Rapportering av IKT-relaterade incidenter (artiklarna 15—20)

Enligt förslaget ska en finansmarknadsaktör även ha allmän skyldighet att övervaka IKT-relaterade incidenter i sin organisation, ta upp och kategorisera dem enligt de europeiska finansmarknadsmyndigheternas kriterier och anmäla incidenterna till en behörig nationell myndighet. Vid betydande incidenter ska aktören informera sina kunder om hur incidenten har påverkat eller kan påverka kundens intressen. Information om IKT-incidenter bör förmedlas mellan myndigheter och finansmarknadsaktörer. De behöriga myndigheterna ska även dela information om betydande incidenter till andra myndigheter. Samtidigt ska de ge aktörer tillsynsfeedback och vägledning om anmälan om incidenter.

3.1.4 Testning av digital operativ motståndskraft (artiklarna 21—24)

Skyldigheten till bastester av digital operativ motståndskraft ska vara tillämplig i alla organisationer. De finansmarknadsaktörer som tillsynsmyndigheten har kategoriserat som betydande ska däremot vara skyldiga att med tre års mellanrum tillämpa omfattande TLPT-tester (*Threat Led Penetration Testing*) som riktas till organisationens IKT-beredskap och IKT-funktioner. Det närmare föremålet för ett test beror på organisationens och tillsynsmyndighetens godkännande.

[8] KOMMISSIONENS REKOMMENDATION av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Behöriga myndigheter ska identifiera och kategorisera finansmarknadsaktörer som betydande aktörer enligt de europeiska finansmarknadsmyndigheternas kriterier.

3.1.5 Tredjepartsrisker (artiklarna 25—39)

I förslaget till förordning (artiklarna 25—27) fastställs huvudsakliga principer som är viktiga i verksamheten med kritiska tredje parter som tillhandahåller IKT-service. Avtalen mellan finansmarknadsaktörer och tredje parter ska innefatta villkor för bland annat följande: servicebeskrivning, ställen där finansmarknadsaktörens data behandlas, servicenivå, kvantitativa och kvalitativa prestationsmål, tredje partens tillgänglighet, säkerhet i personuppgifter, skydd och återställande, tredje partens skyldighet att ge information till exempel vid driftstörningar samt uppsägningsrätt och exitstrategier. Finansmarknadsaktörer och myndigheter ska även ha tillgång till och rätt till insyn i tredje partens data. De minimikrav som ska fastställas i lagstiftningen ska stödja finansmarknadsaktörernas kapacitet att på ett effektivt sätt övervaka riskerna i verksamheten med stora tjänsteleverantörer.

I förslaget fastställs även en tillsynsram som ska tillämpas på tredje parter (artiklarna 28—39). Tillsynsramen ska bestå av ett tillsynsforum som i sin tur utgörs av en gemensam kommitté bestående av de europeiska finansmarknadsmyndigheterna och underkommittéer. Till medlemmarna av tillsynsforum hör även en företrädare för varje nationell behörig myndighet och observatörer från bland annat Europeiska centralbanken. Forum ska samordna IKT-risker med tredje parter, utföra tillsynsarbete och ge rekommendationer utifrån sina observationer. En huvudtillsynsmyndighet ska utnämnas för varje kritisk tredje part och huvudtillsynsmyndigheten ska vara en av de tre europeiska finansmarknadsmyndigheterna.

3.1.6 Informationsutbyte och informationsdelning (artikel 40)

Förslaget ska även möjliggöra frivilligt informationsutbyte mellan finansmarknadsaktörer vid cyberhot. Informationsutbytet ska uppmuntra aktörerna att utnyttja den egna kollektiva kännedomen och praktiska erfarenheten på strategisk, taktisk och operativ nivå. På så sätt ska aktörerna ha en bättre kapacitet att på ett effektivare sätt bedöma cyberhot, följa upp hur hoten utvecklas, försvara sig mot hoten och åtgärda hoten.

3.1.7 Behöriga myndigheter (artiklarna 41—43, 47 och 49)

De behöriga myndigheter som har utnämnts i unionens gällande sektorspecifika finansmarknadslagstiftning ska i princip också vara de behöriga myndigheter som avses i förslaget, och ha den behörighet som krävs i bestämmelserna. I Finland är dessa myndigheter Finansinspektionen för organisationer som är verksamma i den finansiella sektorn och Patent- och registerstyrelsen för revisorer. Dessutom står systemviktiga finansmarknadsaktörer och infrastrukturer under tillsyn av nationella centralbanker. Bestämmelserna för behöriga myndigheter ska även innefatta bestämmelser om yrkesmässig sekretess, samarbete och informationsutbyte.

3.1.8 Sanktioner (artiklarna 44—46 och 48)

Medlemsstaterna ska även se till att de nationella myndigheterna har lämpliga behörigheter för att ingripa i överträdelser av förordningen i form av sanktioner.

3.1.9 Utövande av delegering (artikel 50)

Kommissionen kan anta delegerade förordningar om definition av kritiska tredje parter (artikel 28) och om tillsynsavgifter (artikel 38).

Förslaget till förordning omfattar även befogenheter för de europeiska finansmarknadsmyndigheterna att ta fram tekniska tillsynsstandarder för bland annat verktyg, metoder, processer och praxis för IKT-riskhantering (artikel 14), rapportering av IKT-relaterade incidenter (artikel 16), testning av IKT-system (artikel 23), allmänna principer som gäller tredje parter (artikel 25), avtal som ingås med tredje parter (artikel 27), kontinuerlig övervakning (artikel 35) och harmonisering av övervakningen av kritiska tredje parter (artikel 36).

3.1.10 Ikraftträdande och slutbestämmelser (artiklarna 51—56)

Efter att förordningen varit i kraft i fem år ska kommissionen se över kriterierna för definition av tredje parter. Förordningen innehåller även de ändringar som har föreslagits för unionens övriga förordningar. Den föreslagna förordningen avses träda i kraft den 20:e dagen efter att den publicerats i Europeiska unionens officiella tidning, och ska börja tillämpas tolv månader efter att den trätt i kraft. Förslaget till direktiv avses träda i kraft den 20:e dagen efter att den publicerats i Europeiska unionens officiella tidning, och ska börja tillämpas tolv månader efter att det trätt i kraft.

3.2 Förslag till kompletterande ändringsdirektiv

Genom direktivet ska ändringar göras i följande direktiv gällande finansmarknadslagstiftning: 2006/43/EG[9], 2009/65/EG[10], 2009/138/EU[11], 2011/61/EU[12], EU/2013/36[13], 2014/65/EU[14], EU/2015/2366[15] och EU/2016/2341[16]. Artiklarna i direktiven ska preciseras genom ändringarna så att motstridigheterna med förslaget till förordning blir raderade. Syftet med förslaget är bland annat att förenkla och harmonisera IKT-riskhanteringen och riskidentifieringen. Förslaget till

[9] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG.
[10] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag).
[11] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II).
[12] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010.
[13] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.
[14] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU.
[15] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.
[16] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut.

direktiv innehåller även ändringar som har samband med förslagen till förordning om kryptotillgångar. Ändringarna behandlas närmare i en separat U-skrivelse.

4 Förslagens rättsliga grund och förhållande till subsidiaritets- och proportionalitetsprinciperna och grundlagen

Förslaget till förordning grundar sig på artikel 114 (Tillnärmning av lagstiftning) i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Förslaget till direktiv grundar sig på artikel 53.1 och 114 i EUF-fördraget. Förslagen behandlas i enlighet med det ordinarie lagstiftningsförfarandet och antas i rådet med kvalificerad majoritet. Statsrådet anser att kommissionens förslag är motiverade med hänsyn till den rättsliga grunden.

Enligt subsidiaritetsprincipen (artikel 5.3 i EU-fördraget) ska åtgärder vidtas på EU-nivå endast om och i den mån som målen för den planerade åtgärden inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av den planerade åtgärdens omfattning eller verkningar, bättre kan uppnås på unionsnivå. När enhetliga regler fastställs för IKT-riskhantering och cybersäkerhet i hela unionens område genom förordning, kan motsvarande mål inte uppnås i tillräcklig utsträckning genom EU-medlemsstaternas nationella lagstiftning. De föreslagna bestämmelserna har inte ansetts stå i strid med subsidiaritetsprincipen. Statsrådet anser att förslagen följer subsidiaritetsprincipen och proportionalitetsprincipen i enlighet med det som konstateras i avsnitt 3.1.1.

Den föreslagna förordningens förhållande till skyddet av personuppgifter och utlämnande av uppgifter framhävs särskilt i samband med det frivilliga informationsutbyte som föreslås i fråga om finansmarknadsaktörer. Enligt förslaget till förordning ska informationsutbytet alltid ske med iakttagande av EU:s allmänna dataskyddsförordning[17] och annan EU-lagstiftning om dataskydd. Enligt förslaget ska den behöriga myndigheten också på sin officiella webbplats utan dröjsmål publicera alla beslut om administrativa påföljder som myndigheten har meddelat. Uppgifterna ska bevaras på webbplatsen i minst fem år från det att de publicerades. Personuppgifter som ingår i en publikation får dock bevaras på den behöriga myndighetens officiella webbplats endast så länge det är motiverat enligt dataskyddslagstiftningen. Förslaget till förordning kan anses vara proportionerligt i fråga om skyddet av personuppgifter, eftersom uppgifter inte bör samlas in, bevaras eller lämnas ut i större mängd eller för längre tid än vad som är nödvändigt med tanke på målen i förslaget till förordning och iakttagandet av bestämmelserna i EU:s allmänna dataskyddsförordning. Enligt kommissionen har det i förslaget på detta vis ställts tillräckliga garantier för förutsättningar för lagring av personuppgifter samt för skydd och övervakning av dem.

Förslaget till förordning innehåller kommissionens befogenhet att anta delegerade förordningar.

Statsrådet anser inte att förslagen strider mot Finlands grundlag eller de instrument för grundläggande rättigheter och mänskliga rättigheter som är bindande för Finland.

5 Förslagens konsekvenser

5.1 Konsekvenser för lagstiftningen

[17] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Det krävs ändringar i den nationella lagstiftningen till följd av förslaget till förordning och ändringarna i det därtill hörande direktivet. På grund av det omfattande tillämpningsområdet enligt förslaget till förordning behöver den nationella lagstiftningen ses över. Översynen rör vissa bestämmelser och eventuellt de författningar på lägre nivå och de av Finansinspektionens föreskrifter som har utfärdats med stöd av bestämmelserna, när bestämmelserna, författningarna eller föreskrifterna gäller aktörer som omfattas av tillämpningsområdet.

En del justeringar behöver göras i bland annat kreditinstitutslagen (610/2014), lagen om investeringstjänster (747/2012), lagen om betalningsinstitut (297/2010), lagen om handel med finansiella instrument (1070/2017), lagen om placeringsfonder (213/2019), lagen om förvaltare av alternativa investeringsfonder (162/2014), lagen om pensionsstiftelser (1774/1995), lagen om försäkringskassor (1164/1992), försäkringsbolagslagen (521/2008), revisionslagen (1141/2015) och lagen om värdeandelssystemet och clearingverksamhet (348/2017). För att tillsynsmyndighetens behörighet att utöva tillsyn ska kunna säkerställas behöver vissa justeringar eventuellt också göras i lagen om Finansinspektionen (878/2008).

5.2 Konsekvenser för ekonomin

Syftet med kommissionens förslag är att förbättra motståndskraften på marknaden och att därigenom förebygga negativa ekonomiska konsekvenser. Åtgärderna för att upprätthålla förtroendet på marknaden gynnar indirekt alla marknadsparter, eftersom det rådande förtroendet på den finansiella marknaden blir ännu mer gediget. Enligt kommissionens beräkningar och antaganden uppgick de eventuella negativa konsekvenserna av cyberincidenterna i den finansiella sektorn för hela världsekonomin under 2018 till 45—654 miljarder US-dollar, av vilket EU:s andel skulle ha uppgått till 2—27 miljarder US-dollar. Med användande av kommissionens antaganden skulle de negativa konsekvenserna av cyberincidenterna för Finland ha uppgått till 2,9—39 miljoner US-dollar under 2018. Kommissionen lyfter fram att en minskning på bara tio procent i dessa konsekvenser innebär en årlig besparing på 200—2700 miljoner US-dollar på EU:s finansiella marknad. I Finland ska besparingen uppgå till 0,29—3,9 miljoner US-dollar.

Tillämpningsområdet för kommissionens förslag till förordning omfattar hundratals finska finansiella aktörer. Det finns stora skillnader i aktörernas affärsverksamheter, strukturer och storlekar. Tillämpningsområdet omfattar till exempel väldigt stora aktörer, såsom värdepapperscentraler och kreditinstitut, och eventuellt väldigt små aktörer, såsom registrerade förvaltare av alternativa fonder.

Kommissionens förslag gör att de finansiella aktörernas kostnader inte enbart ökar, utan eventuellt även minskar. Det är svårt att göra några bedömningar av konsekvenser för enskilda företag eller sektorer. De företag som är verksamma inom den finansiella sektorn i Finland har främst ålagts skyldighet att beakta cyberrisker som ett led i hanteringen av operativ risk, och företagen har tagit fram processer för att reagera på riskerna. En del krav på aktörer som omfattas av tillämpningsområdet kommer dock som nya.

Enligt kommissionens bedömning kan förslaget till förordning om digital operativ motståndskraft i den finansiella sektorn medföra både engångskostnader och löpande kostnader för de företag som omfattas av tillämpningsområdet. Engångskostnader orsakas till exempel av de ändringar som behöver göras i olika system till följd av förslaget till förordning. Det är svårt att beräkna olika aktörers kostnader för investeringar i it-system, eftersom aktörernas nuvarande system skiljer sig från varandra. Flera finska aktörer har redan förbättrat den operativa krishanteringskapaciteten och även gjort investeringar i IKT-system, och därför kan kostnaderna för de åtgärder som enligt förslaget ska genomföras bli små. Stora investeringskostnader kan dock

orsakas vissa finska aktörer för anpassning av system efter kraven i förslaget, om kraven inte är tillämpliga i systemen. Enligt kommissionen medför underhåll och testning av IKT-system löpande kostnader för de aktörer som omfattas av tillämpningsområdet. Enligt kommissionens beräkning varierar kostnaderna för testning mellan 0,1 procent och 0,3 procent av ett företags IKT-budget. Enligt kommissionens beräkning kan kostnaderna för rapportering av incidenter till och med minska när vissa överlappande skyldigheter som bygger på olika lagar upphör. Det är sannolikt att konsekvenserna för de finska aktörerna motsvarar kommissionens beräkning.

De kostnader som orsakas små företag förväntas vara låga, eftersom kraven på små företag är mindre strikta på grund av mindre risker. Till följd av tillämpningen av proportionalitetsprincipen ska kraven på små och medelstora företag ställas med hänsyn till bland annat affärsmodeller, storlek, riskprofil och betydelse för systemen. Kraven på anmälan om farliga situationer och på testning är till exempel inte lika strikta för små finansmarknadsaktörer, och därför beräknas kostnaderna för små aktörer vara mindre.

Enligt kommissionens bedömning ska lagstiftningsförslaget inte enbart medföra kostnadseffekter på finansföretag, utan även på tredje parter som tillhandahåller IKT-service. Tillsynen över sådana aktörer kommer att förbättras av tillsynsmyndigheterna, och därför är aktörerna troligen tvungna att ändra den egna verksamheten till de delar det behövs.

För de nationella tillsynsmyndigheterna föreslås nya tillsynsuppgifter. Den gällande lagstiftningen om Finansinspektionen omfattar dock redan nu tillsynsskyldigheter som i hög grad liknar de föreslagna riskhanterings- och rapporteringsskyldigheterna. Till följd av de nya föreslagna uppgifterna och det lite mer omfattande tillämpningsområdet bedöms dock Finansinspektionens arbete öka i någon mån. Den tillsynsmyndighet som övervakar revisorer är revisionstillsyn, som är underställd Patent- och registerstyrelsen. Patent- och registerstyrelsens riskhanterings- och rapporteringsskyldigheter som gäller revisorer bedöms öka till följd av förslagen till förordning. Till följd av de föreslagna nya uppgifterna bedöms Patent- och registerstyrelsens arbete öka i någon mån.

Nya tillsynsuppgifter föreslås även för de europeiska finansmarknadsmyndigheterna. För att utföra de nya uppgifterna behövs sammanlagt 18 nya heltidsanställda, som enligt kommissionens beräkning ska medföra en kostnad på 15 miljoner euro 2022—2027. Dessutom orsakas de europeiska finansmarknadsmyndigheterna andra kostnader för ökningen av tillsynsuppgifterna, men kostnaderna kommer att täckas med tillsynsavgifter. Kostnaderna för ökningen av personalstyrkan ska täckas med medel ur de europeiska finansmarknadsmyndigheternas budgetar.

Lagstiftningsförslagen förbättrar motståndskraften på den finansiella marknaden och det rådande förtroendet på marknaden. Investerare och konsumenter får tillträde till en ännu mer sammanhållen finansiell marknad. Det är dock viktigt att beakta att det troligen är kunderna som får betala en del av kostnadsökningen i form av höjda kund- och serviceavgifter, om de finansiella aktörernas kostnader ökar betydligt på grund av lagstiftningsförslagen.

6 Den nationella behandlingen av förslagen och behandlingen i Europeiska unionen

Förslagen och utkastet till statsrådets skrivelse som hänför sig till dem var ute på remiss i ett skriftligt förfarande i sektionen för finansiella tjänster och kapitalrörelser (sektion 10) under kommittén för EU-ärenden mellan den 19 och den 26 oktober 2020.

Behandlingen av förslagen inleddes på det första mötet för arbetsgruppen för finansiella tjänster den 30 september 2020. Det tyska ordförandeskapet har meddelat att dess mål är att bidra till en effektiv behandling av förslagen i höst. De andra medlemsstaternas ståndpunkter är ännu inte kända.

7 Ålands behörighet

Ärendet omfattas av rikets lagstiftningsbehörighet enligt 27 § i självstyrelselagen för Åland (1144/1991).

8 Statsrådets ståndpunkt

Statsrådet förenar sig med kommissionens syn på att tillgången till innovativa finansiella tjänster för företag och konsumenter behöver främjas. En utökning av konkurrensvillkoren främjar möjligheten för den finansiella tjänstesektorn att förnya sig och bidrar till att skapa nya affärsmodeller. Samtidigt ska de risker som uppstår till följd av digitaliseringen kunna identifieras, och det är motiverat att delvis ingripa i riskerna även genom en enhetlig lagstiftning för unionen. Åtgärderna för att förbättra den digitala operativa motståndskraften i den finansiella sektorn är goda för att servicen ska fungera väl och stabiliteten i den finansiella sektorn ska kunna säkerställas. I framtiden är det därför allt viktigare med en noggrannare tillsyn över alla aktörers cybersäkerhetsberedskap.

Statsrådet välkomnar de mål som i förslagen till förordning och direktiv föreslås i syfte att harmonisera och strömlinjeforma bestämmelserna om IKT-riskhantering och cybersäkerhet i unionens lagstiftning om den inre marknaden. De föreslagna reglerna fastställer de enhetliga principerna för kontinuitetshantering i finansmarknadsaktörernas affärsverksamhet, främjar tillsynen över kritiska icke-finansiella tjänsteleverantörer och skapar ramar för utnyttjande av teknisk innovation. När regelverket om unionens finansiella marknad stärks, ska hänsyn emellertid tas till arrangemangen för att säkerställa de finansiella tjänster som är kritiska för den nationella säkerheten. Enligt grundfördragen är varje medlemsstat fortsatt ansvarig för den nationella säkerheten.

Statsrådet stöder tillämpningen av den proportionalitetsprincip som föreslås i förslaget och som möjliggör hänsyn till olika aktörers särdrag. Tillämpningen av proportionalitetsprincipen ska dock kunna bedömas noggrant med tanke på befintliga risker. Statsrådet stöder förslaget till skapande av en intern ram för riskhantering i organisationer och till kontinuerlig utveckling av ramen. Dessutom anser statsrådet att det är lönt att understödja förslagens mål om att genom förslagen harmonisera och specificera de krav som de finansiella aktörerna åtminstone ska beakta när de ingår avtal med kritiska tredje parter.

Statsrådet anser att det är godtagbart att inrätta en sådan ny tillsynsram på övre nivån som föreslås i förslaget till förordning, förutsatt att ramen är avsedd att stärka tillsynen över tredje parter. Statsrådet förhåller sig emellertid förbehållsamt till ramens administrationsstruktur. I administrationsstrukturen bör hänsyn tas till att behörigheterna och ansvarsfördelningen är tydliga för både de nationella behöriga myndigheterna och de europeiska finansmarknadsmyndigheterna. En förutsättning för genomförande av projekt för harmonisering av den europeiska regleringen är att myndigheternas behörigheter ska vara entydiga och tillräckliga.

I förslagen vill statsrådet även fästa uppmärksamhet på det ändamålsenliga informationsutbytet mellan olika myndigheter. Förslagen bör bidra till att förbättra informationsutbytet mellan olika

myndigheter och möjliggöra omständigheter som inte utgör något hinder för informationsutbytet, framför allt i krislägen.

Dessutom understryker statsrådet att det är viktigt att säkerställa motståndskraften i den finansiella sektorn genom att även i unionens verksamhet ta fram handlingsmodeller baserat på ett systemiskt övergripande säkerhetstänkande. Det är viktigt att säkerställa myndigheternas insatser framför allt i anslutning till vidsträckta störningar. I den fortsatta behandlingen av förslagen ska uppmärksamhet därför ägnas åt att rapporteringen av störningar är ordnad på ett ändamålsenligt sätt och att informationsutbytet mellan olika myndigheter säkerställs på ett lämpligt sätt.

Förslaget till förordning omfattar kommissionens befogenhet att anta delegerade akter. Statsrådet anser att delegerade akter till sin karaktär främst är tekniska bestämmelser och att befogenheterna utifrån statsrådets bedömning därför också kan godkännas.