RP 67/2024 rd

Regeringens proposition till riksdagen med förslag till lag om ändring av lagen om Finansinspektionen och till vissa lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att lagen om Finansinspektionen, kreditinstitutslagen, lagen om investeringstjänster, lagen om betalningsinstitut, lagen om handel med finansiella instrument, lagen om placeringsfonder, lagen om förvaltare av alternativa investeringsfonder, lagen om tilläggspensionsstiftelser och tilläggspensionskassor, försäkringsbolagslagen, lagen om aktiebolaget Fonden för industriellt samarbete Ab och lagen om statens specialfinansieringsbolag ändras.

Syftet med propositionen är att utfärda nationella bestämmelser som kompletterar EU:s så kallade DORA-förordning om digital operativ motståndskraft för finanssektorn, att genomföra det så kallade DORA-ändringsdirektivet om ändring av vissa direktiv vad gäller digital operativ motståndskraft för finanssektorn samt att utfärda bestämmelser som kompletterar det nationella genomförandet av det så kallade NIS 2-direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och av det så kallade CER-direktivet om kritiska entiteters motståndskraft när det gäller bankverksamhet och finansmarknadsinfrastruktur.

I lagen om Finansinspektionen föreslås det bestämmelser om att Finansinspektionen ska vara behörig myndighet enligt EU:s DORA-förordning samt behörig myndighet enligt NIS 2-direktivet och CER-direktivet när det gäller bankverksamhet och finansmarknadsinfrastruktur. Finansinspektionens uppgifter utvidgas så att den också har till uppgift att främja cybersäkra tillvägagångssätt hos finansmarknadsaktörer samt främja kritiska finansmarknadsaktörers motståndskraft. Finansinspektionens skyldigheter att samarbeta med andra myndigheter i syfte att främja cybersäkerheten föreslås bli samlade i en ny paragraf. Dessutom föreslås det att lagens bestämmelser om administrativa påföljder kompletteras med anledning av EU:s DORA-förordning och att de tredjepartsleverantörer av informations- och kommunikationstekniktjänster som omfattas av förordningens tillämpningsområde läggs till i förteckningen över i lagen avsedda andra finansmarknadsaktörer.

Lagen om aktiebolaget Fonden för industriellt samarbete Ab och lagen om statens specialfinansieringsbolag föreslås bli ändrade så att Fonden för industriellt samarbete Ab och Finnvera Abp lämnas utanför tillämpningsområdet för EU:s DORA-förordning.

När det gäller de övriga lagar som föreslås bli ändrade förutsätter DORA-ändringsdirektivet att det till lagen fogas bestämmelser om krav på att förvalta nätverks- och informationssystem i enlighet med EU:s DORA-förordning samt vissa andra ändringar.

De föreslagna lagarna avses träda i kraft den 17 januari 2025.

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Europaparlamentet och rådet antog den 14 december 2022 förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (nedan *EU:s DORA-förordning*). Förordningen offentliggjordes i Europeiska unionens officiella tidning den 27 december 2022 och trädde i kraft den tjugonde dagen efter offentliggörandet, den 16 januari 2023. Förordningen ska tillämpas från och med den 17 januari 2025. Medlemsstaterna ska senast den 17 januari 2025 offentliggöra de nationella lagändringar som är nödvändiga för att genomföra förordningen. I samma nummer av Europeiska unionens officiella tidning offentliggjordes Europaparlamentets och rådets direktiv (EU) 2022/2556 om ändring av direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341 vad gäller digital operativ motståndskraft för finanssektorn (nedan *DORA-ändringsdirektivet*), som liksom EU:s DORA-förordning trädde i kraft den tjugonde dagen efter offentliggörandet, det vill säga den 16 januari 2023. Medlemsstaterna ska senast den 17 januari 2025 anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet.

EU:s DORA-förordning och DORA-ändringsdirektivet ingår i Europeiska kommissionens åtgärdspaket för att ytterligare möjliggöra och stödja den digitala finanssektorns potential när det gäller innovation och konkurrens, skapa nya alternativ jämsides med befintliga finansiella tjänster och betaltjänster och samtidigt minska riskerna. I paketet ingår en ny strategi för digitalisering av finanssektorn, vars syfte är att främja nivån av digitalisering inom EU:s finanssektor och se till att europeiska konsumenter och företag gynnas av den.

I paketet för digitalisering av finanssektorn ingår förutom EU:s DORA-förordning, DORA-ändringsdirektivet och strategin för digitalisering av finanssektorn en förordning om marknader för kryptotillgångar och en pilotordning för marknadsinfrastrukturer som bygger på teknik för distribuerade liggare.

Utöver EU:s DORA-förordning och DORA-ändringsdirektivet antog Europaparlamentet och rådet den 14 december 2022 direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (nedan *NIS 2-direktivet*) samt direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (nedan *CER-direktivet*). Eftersom den digitala motståndskraften hos finansbranschaktörer regleras på ett övergripande sätt i EU:s DORA-förordning bör de skyldigheter som följer av NIS 2- och CER-direktiven inte tillämpas på de finansbranschaktörer som omfattas av de direktiven för att undvika överlappande reglering och onödig administrativ börda. Det är dock viktigt att dessa aktörer beaktas i de nationella strategier och åtgärder som avses i dessa direktiv och i samarbetsstrukturerna mellan myndigheter för att säkerställa samstämmigheten med bland annat de cybersäkerhetsstrategier som medlemsstaterna antagit och informationsflödet mellan myndigheterna.

1.2 Beredning

Beredningen av EU-rättsakten

Kommissionen offentliggjorde den 24 september 2020 ett förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014 samt ett förslag till Europaparlamentets och rådets direktiv om ändring av direktiven 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 216/2341. Samtidigt offentliggjorde kommissionen också förslag till Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av direktiv (EU) 2019/1937 (*MiCA*) och Europaparlamentets och rådets förordning om en pilotordning för marknadsinfrastrukturer som baseras på teknik för distribuerade liggare (*DLT-pilotordningen*). Förslagen till rättsakter ingår i kommissionens paket för digitalisering av finanssektorn (COM(2020) 591 final).

Kommissionens förslag till förordning och direktiv samt utkastet till statsrådets skrivelse till riksdagen om kommissionens förslag var i oktober 2020 på remiss i sektionen för finansiella tjänster och kapitalrörelser (EU-10), som lyder under kommittén för EU-ärenden. En U-skrivelse (U 58/2020 rd) om kommissionens förslag lämnades till riksdagen. Behandlingen av förslagen inleddes i rådets arbetsgrupp för finansiella tjänster den 30 september 2020.

Statsrådet förhöll sig positivt till förslagen och instämde med kommissionens uppfattning att det är viktigt att förbättra den digitala operativa motståndskraften i den finansiella sektorn för att servicen ska fungera väl och stabiliteten i den finansiella sektorn ska kunna säkerställas. Statsrådet välkomnade förordningens mål om harmonisering av bestämmelserna om riskhantering inom informations- och kommunikationsteknik (*nedan* IKT) och cybersäkerhet, men när regelverket stärks ska hänsyn tas till arrangemangen för att säkerställa de finansiella tjänster som är kritiska för den nationella säkerheten.

Statsrådet understödde tillämpningen av den föreslagna proportionalitetsprincipen så länge tillämpningen övervägs noggrant med tanke på befintliga risker. Statsrådet ansåg att det är godtagbart att inrätta den föreslagna nya tillsynsramen på en övre nivå, men förhöll sig avvaktande till ramens administrationsstruktur. Statsrådet påpekade att det i administrationsstrukturen bör tas hänsyn till att behörigheterna och ansvarsfördelningen ska vara tydliga mellan de nationella och europeiska myndigheterna.

Rapporteringen av störningar och informationsgången mellan myndigheterna ska ordnas på ett ändamålsenligt sätt, vilket enligt statsrådet bör uppmärksammas i den fortsatta beredningen av förslaget. Statsrådet underströk bland annat att det är viktigt att i unionens verksamhet ta fram handlingsmodeller baserade på ett systemiskt övergripande säkerhetstänkande.

Riksdagens ekonomiutskott omfattade statsrådets ståndpunkt med särskild tonvikt på vissa synpunkter (EkUU 26/2020 rd). I fråga om proportionalitetsprincipen påpekade ekonomiutskottet att det är väsentligt att bedöma uttryckligen aktörens påverkan på marknaden och inte enbart aktörens storlek, eftersom ett problem med omfattande konsekvenser också kan få sin början från en liten aktör som försummar sin riskhantering. Dessutom påpekade ekonomiutskottet att kontaktytan mellan en långtgående harmoniserad europeisk reglering av den finansiella sektorn och regleringen för att säkerställa den nationella säkerheten är en kritisk punkt för att lagstiftningens mål ska kunna uppnås.

Beredningen av propositionen

Regeringens proposition bereddes som tjänsteuppdrag vid finansministeriet. I arbetet deltog också social- och hälsovårdsministeriet. Utkastet till proposition var på remiss 19.2–29.3.2024.

Yttranden lämnades av 16 instanser. I avsnitt 6 redogörs för remissvaren och hur de har beaktats i regeringens proposition.

Beredningsunderlaget till propositionen finns i den offentliga tjänsten under adressen valtioneuvosto.fi/sv/projekt med identifieringskod VM067:00/2023.

2 EU-rättsaktens målsättning och huvudsakliga innehåll

Allmänna bestämmelser

I kapitel I i EU:s DORA-förordning finns allmänna bestämmelser om förordningens innehåll, tillämpningsområde och definitioner och om proportionalitetsprincipen.

I syfte att uppnå en hög gemensam nivå av digital operativ motståndskraft fastställs i förordningen enhetliga krav avseende säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser. I artikel 2 i förordningen finns bestämmelser om förordningens tillämpningsområde. Förordningen tillämpas på aktörer som anges närmare i artikel 2.1 a–t, och som tillsammans benämns finansiella entiteter, och på tredjepartsleverantörer av IKT-tjänster. Förordningen tillämpas inte på förvaltare av alternativa investeringsfonder som avses i artikel 3.2 i direktiv 2011/61/EU, försäkrings- och återförsäkringsföretag som avses i artikel 4 i direktiv 2009/138/EG, tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 15 medlemmar, fysiska eller juridiska personer som är undantagna enligt artiklarna 2 och 3 i direktiv 2014/65/EU, försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet som är mikroföretag eller små eller medelstora företag samt postgiroinstitut som avses i artikel 2.5.3 i direktiv 2013/36/EU. Medlemsstaterna får från tillämpningsområdet utesluta sådana enheter som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU om de är belägna inom deras respektive territorier. Finland får alltså besluta att inte tillämpa förordningen på Fonden för industriellt samarbete Ab och Finnvera Abp.

Med digital operativ motståndskraft avses i förordningen en finansiell entitets förmåga att bygga upp, säkerställa och se över sin operativa integritet och tillförlitlighet genom att, direkt eller indirekt, med användning av tjänster från tredjepartsleverantörer av IKT-tjänster, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell entitet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet, inbegripet under avbrott. IKT-risk definieras i förordningen som varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem som, om de inträffar, kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är teknikberoende, funktioner och processer eller tillhandahållandet av tjänster genom att orsaka negativa effekter i den digitala eller fysiska miljön. För definitioner av nätverks- och informationssystem och deras säkerhet hänvisas det i förordningen till definitionerna i NIS 2-direktivet. Med cyberhot avses definitionen i artikel 2.8 i förordning (EU) 2019/881, nämligen en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat sätt negativt påverka nätverks- och informationssystem, användare av dessa system och andra personer.

I artikel 4 i förordningen föreskrivs det om proportionalitetsprincipen. Enligt artikeln ska skyldigheterna i förordningen tillämpas i enlighet med proportionalitetsprincipen så att de står i proportion till entiteternas storlek och allmänna riskprofil och karaktären på, omfattningen av och komplexiteten i deras tjänster, verksamhet och insatser. I artikeln krävs också att de

behöriga myndigheterna ska beakta finansiella entiteters tillämpning av proportionalitetsprincipen i sin översyn.

IKT-riskhantering

Kapitel II i förordningen innehåller bestämmelser om IKT-riskhantering. Enligt artikel 5 i förordningen ska finansiella entiteter ha en intern styrnings- och kontrollram som säkerställer en effektiv och ansvarsfull hantering av IKT-risk i syfte att upprätthålla en hög nivå av digital operativ motståndskraft. Den finansiella entitetens ledningsorgan ska sköta alla arrangemang som rör IKT-riskhanteringen och övervaka och ansvara för dem.

Närmare bestämmelser om innehållet i IKT-riskhanteringen finns i avsnitt II i kapitel II i förordningen. I artikel 6 i förordningen föreskrivs det att finansiella entiteter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram som en del av sitt övergripande riskhanteringssystem. I artikeln finns bestämmelser om innehållskrav för IKT-riskhanteringsramen, uppdaterad information till myndigheterna, överföring av ansvaret för övervakningen till en separat kontrollfunktion, dokumentation och översyn av ramen samt internrevision och en intern uppföljningsprocess för den. IKT-riskhanteringsramen ska omfatta en strategi för digital operativ motståndskraft som inbegriper särskilda i artikeln specificerade metoder för att uppnå IKT-mål.

I artikel 7 i förordningen finns bestämmelser om en skyldighet för finansiella entiteter att upprätthålla IKT-system, IKT-protokoll och IKT-verktyg som är lämpliga, tillförlitliga, har tillräcklig kapacitet och är tekniskt motståndskraftiga för att hantera stora informationsvolymer vid behov. Som en del av IKT-riskhanteringen ska finansiella entiteter enligt artikel 8 identifiera, klassificera och dokumentera alla IKT-stödda affärsfunktioner, roller och ansvarsområden, de informationstillgångar och IKT-tillgångar som stöder dessa funktioner och deras roller och beroenden i förhållande till IKT-risk. Kravet på identifiering gäller också källor till IKT-risk, informations- och IKT-tillgångar, nätverksresurser och maskinvaruutrustning samt processer som är beroende av tredjepartsleverantörer av IKT-tjänster och kopplingar till dem.

Enligt artikel 9 i förordningen ska finansiella entiteter kontinuerligt övervaka och kontrollera IKT-systemens funktion och minimera effekterna av relaterade risker på systemens funktionsförmåga. Finansiella entiteter ska ha IKT-relaterade säkerhetsförfaranden och verktyg för att säkerställa höga standarder för systemens motståndskraft, kontinuitet och tillgänglighet. Finansiella entiteter ska ha mekanismer för att snabbt upptäcka IKT-relaterade incidenter, och de ska innehålla vissa fastställda varningströskelvärden och varningskriterier för att inleda processer i samband med IKT-relaterade incidenter. Enligt artikel 11 i förordningen ska finansiella entiteter införa en policy för att säkerställa kontinuiteten i deras kritiska eller viktiga funktioner, reaktionen på samt återställandet efter IKT-relaterade incidenter. Finansiella entiteter ska ha lämpliga IKT-kontinuitetsplaner samt IKT-åtgärds- och återställningsplaner som ska testas årligen. I det syftet ska finansiella entiteter också inrätta förfaranden och system för säkerhetskopiering och återskapande.

Enligt artikel 13 i förordningen ska IKT-riskhanteringen kontinuerligt ses över och efter allvarliga IKT-relaterade incidenter ska en efterhandsöversyn ordnas där man analyserar orsaken och identifierar hur man kan bättre kan reagera på incidenter och utveckla IKT-riskhanteringsramen. Enligt artikel 14 ska finansiella entiteter också ha kriskommunikationsplaner som gör det möjligt att effektivt informera kunder och motparter samt allmänheten.

Enligt artikel 15 ska de europeiska tillsynsmyndigheterna utarbeta förslag till tekniska standarder för tillsyn i fråga om de aspekter som räknas upp i artikeln för att harmonisera verktyg, metoder, processer och strategier för IKT-riskhantering. Till kommissionen delegeras befogenhet att komplettera förordningen genom att anta de ovannämnda tekniska standarderna för tillsyn. I artikel 16 i förordningen finns bestämmelser om krav på en förenklad IKT-riskhanteringsram för vissa finansiella entiteter.

Hantering av, klassificering av och rapportering om IKT-relaterade incidenter

I kapitel III i förordningen finns bestämmelser om finansiella entiteters skyldighet att hantera, klassificera och rapportera om IKT-relaterade incidenter. Enligt artikel 17 ska entiteter fastställa, inrätta och genomföra en hanteringsprocess för att upptäcka, hantera och rapportera vidare om IKT-relaterade incidenter. Alla IKT-relaterade incidenter och betydande cyberhot ska registreras. Finansiella entiteter ska också klassificera IKT-relaterade incidenter och fastställa deras inverkan enligt kriterier som närmare anges i artikel 18.1 a–f. Till dessa kriterier hör bland annat incidentens varaktighet, den geografiska spridningen av de områden som påverkas samt de berörda tjänsternas kritikalitet.

Enligt artikel 19 är finansiella entiteter skyldiga att rapportera allvarliga IKT-relaterade incidenter till den relevanta behöriga myndighet som avses i förordningen. Dessa inbegriper bland annat nationella myndigheter enligt NIS 2-direktivet och resolutionsmyndigheter. Dessutom har finansiella entiteter enligt förordningen möjlighet att frivilligt rapportera betydande cyberhot till den behöriga myndigheten. Beroende på om det är fråga om skyldighet eller frivillighet ska eller får den behöriga myndighet som tar emot informationen lämna den vidare till andra myndigheter. De europeiska tillsynsmyndigheterna ska utarbeta förslag till tekniska standarder bland annat för väsentlighetströsklar för IKT-relaterade incidenter och innehållet i rapporteringen, och till kommissionen delegeras befogenhet att komplettera förordningen genom att anta de nämnda tekniska standarderna.

Testning av digital operativ motståndskraft

I kapitel IV i förordningen finns bestämmelser om testning av digital operativ motståndskraft. Finansiella entiteter ska införa heltäckande program för testning av digital operativ motståndskraft och följa en riskbaserad metod när de genomför programmet. Enligt artikel 26 i förordningen ska vissa särskilt identifierade finansiella entiteter minst vart tredje år genomföra avancerade tester med hjälp av hotbildsstyrd penetrationstestning som omfattar flera eller alla av den finansiella entitetens kritiska eller viktiga funktioner. Dessutom föreskrivs det om krav för testare som anlitas för att utföra hotbildsstyrd penetrationstestning.

Hantering av IKT-tredjepartsrisker

I kapitel V i förordningen finns bestämmelser om hantering av IKT-tredjepartsrisker. I avsnitt 1 i kapitlet finns bestämmelser om huvudprinciper för en sund hantering av IKT-tredjepartsrisker. Finansiella entiteter ska hantera IKT-tredjepartsrisker enligt de allmänna principer som anges i artikel 28 och anta en strategi för IKT-tredjepartsrisk. Artikeln innehåller också krav som gäller kontraktsmässiga arrangemang om användning av IKT-tjänster. Den behöriga myndigheten ska informeras på förhand om planerade kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner. När det gäller IKT-tjänster som stöder kritiska eller viktiga funktioner ska finansiella entiteter införa exitstrategier. Enligt artikel 29 i förordningen ska finansiella entiteter när de utför den identifiering och bedömning av risk som avses i artikel 28.4 c även ta hänsyn till de risker som

kan uppstå om upphandlingen av IKT-tjänster koncentreras till en och samma eller nära anknutna tjänsteleverantörer. I det sammanhanget måste finansiella entiteter överväga olika alternativ, till exempel om IKT-tjänster borde upphandlas från flera olika tjänsteleverantörer för att minimera koncentrationsrisken. Artikel 30 i förordningen innehåller viktiga avtalsbestämmelser i avtal mellan finansiella entiteter och tredjepartsleverantörer av IKT-tjänster.

I avsnitt II i kapitlet finns bestämmelser om en tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster. I förordningen åläggs de europeiska tillsynsmyndigheterna att klassificera tredjepartsleverantörer av IKT-tjänster som kritiska för finansiella entiteter och utse en ledande tillsynsmyndighet för varje kritisk tredjepartsleverantör. De europeiska tillsynsmyndigheterna är Europeiska bankmyndigheten (EBA) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1093/2010, Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1094/2010 samt Europeiska värdepappers- och marknadsmyndigheten (Esma) inrättad genom förordning (EU) nr 1095/2010. Klassificeringen ska baseras på bland annat betydelsen för systemet av de finansiella entiteter som är beroende av den berörda tredjepartsleverantören av IKT-tjänster. Klassificering av kritiska tjänsteleverantörer tillämpas inte på tredjepartsleverantörer av IKT-tjänster som endast tillhandahåller IKT-tjänster i en medlemsstat till finansiella entiteter som endast är verksamma i den medlemsstaten. I artikel 32 finns bestämmelser om tillsynsramens struktur. Den gemensamma kommittén ska inrätta ett tillsynsforum som en underkommitté med uppgiften att stödja arbetet i den ledande tillsynsmyndigheten för de kritiska tredjepartsleverantörerna av IKT-tjänster. Tillsynsforumet består av de aktörer som anges i artikel 32.4 a–e. Från varje medlemsstat ska en företrädare på hög nivå för den tjänstgörande personalen på den relevanta behöriga myndighet som avses i förordningens artikel 46 delta i tillsynsforumet, och när så är lämpligt, ytterligare en företrädare från en behörig myndighet som avses i artikel 46 i varje medlemsstat som observatör. Medlemsstaterna ska utse och informera den ledande tillsynsmyndigheten om den myndighet vars anställde ska vara den ovan avsedda företrädaren på hög nivå.

Den ledande tillsynsmyndighet som utsetts i enlighet med artikel 31 ska enligt de uppgifter som anges i artikel 33 utöva tillsyn över de kritiska tredjepartsleverantörer av IKT-tjänster som den tilldelats. Den ledande tillsynsmyndigheten ska bedöma huruvida varje kritisk tredjepartsleverantör av IKT-tjänster har infört heltäckande, sunda och effektiva regler, förfaranden, mekanismer och arrangemang för att hantera den IKT-risk som den kan medföra för finansiella entiteter. Tillsynen samordnas inom ramen för det gemensamma tillsynsnätverk som inrättas med stöd av artikel 34. I artikel 35 i förordningen finns bestämmelser om den ledande tillsynsmyndighetens befogenheter för att fullgöra sina föreskrivna uppgifter. Den ledande tillsynsmyndigheten har bland annat befogenheter att begära all relevant information och dokumentation i enlighet med artikel 37 samt genomföra allmänna utredningar och inspektioner i enlighet med artiklarna 38 respektive 39. En av den ledande tillsynsmyndighetens befogenheter är att förelägga en tredjepartsleverantör av IKT-tjänster med vite för bristande efterlevnad av de åtgärder den ska vidta. Enligt punkt 9 i artikeln ska vitet vara av administrativ karaktär och verkställbart. Verkställigheten ska följa de regler som gäller i den medlemsstat inom vars territorium inspektionerna av och åtkomsten till tredjepartsleverantörs lokaler ska genomföras. Domstolarna i den berörda medlemsstaten ska vara behöriga att pröva klagomål som rör oegentligheter i verkställigheten.

I artikel 36 i förordningen finns bestämmelser om den ledande tillsynsmyndighetens befogenheter i situationer då utövandet av befogenheterna riktar sig mot lokaler i tredjeländer som ägs eller används av en kritisk tredjepartsleverantör av IKT-tjänster till finansiella entiteter i unionen och har samband med leverantörens affärsverksamhet, funktioner eller tjänster.

Bestämmelser om befogenheter finns i artikel 35.1 a–b, artikel 38.2 a, b och d samt artikel 39.1 och 39.2 a. För att dessa bestämmelser ska kunna tillämpas måste EBA, Esma eller Eiopa ingå arrangemang för administrativt samarbete med de relevanta myndigheterna i tredjelandet för att den ledande tillsynsmyndigheten på ett smidigt sätt ska kunna utöva sina befogenheter i samarbete med den grupp som utsetts i det berörda tredjelandet. Enligt artikel 36 får det som nämns ovan inte påverka unionsinstitutionernas eller medlemsstaternas befogenheter eller medföra några rättsliga skyldigheter för unionen eller medlemsstaterna. Agerandet får inte heller hindra medlemsstaterna och deras behöriga myndigheter från att ingå bilaterala eller multilaterala arrangemang med tredjeländer och deras relevanta myndigheter.

Enligt artikel 40 i förordningen ska den ledande tillsynsmyndigheten vid tillsynsåtgärderna bistås av en gemensam undersökningsgrupp som har inrättats för varje kritisk tredjepartsleverantör av IKT-tjänster. Närmare bestämmelser om gruppens sammansättning finns i artikel 40.2 a–d. Till undersökningsgruppen hör från medlemsstaterna de relevanta behöriga myndigheter som utövar tillsyn över de finansiella entiteter till vilka den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller IKT-tjänster samt på frivillig basis en nationell behörig myndighet från den medlemsstat där den kritiska tredjepartsleverantören av IKT-tjänster är etablerad. Inom 60 kalenderdagar från mottagandet av de rekommendationer som har utfärdats av den ledande tillsynsmyndigheten enligt artikel 35.1 d ska kritiska tredjepartsleverantörer av IKT-tjänster antingen underrätta den ledande tillsynsmyndigheten om sin avsikt att följa rekommendationerna eller lämna en motiverad förklaring till varför de inte följer sådana rekommendationer. I artikel 42 i förordningen finns bestämmelser om behöriga myndigheters uppföljning i sådana situationer. Som en sista utväg får de behöriga myndigheterna fatta ett beslut om att finansiella entiteter tillfälligt, helt eller delvis, ska avbryta användningen eller införandet av en tjänst som tillhandahålls av den kritiska tredjepartsleverantörer av IKT-tjänster eller kräva att finansiella entiteter helt eller delvis ska avsluta de kontraktsmässiga arrangemang som har ingåtts med de kritiska tredjepartsleverantörerna av IKT-tjänster.

Arrangemang för informationsutbyte

I förordningen föreskrivs om en möjlighet för finansiella entiteter att sinsemellan utbyta information och underrättelser om cyberhot, i den mån utbyte av denna information uppfyller de kriterier som anges i artikel 45.1 a–c i DORA-förordningen. Arrangemangen för informationsutbyte ska innehålla fastställda villkor för deltagande och närmare uppgifter om offentliga myndigheters deltagande och på vilket sätt dessa kan knytas till arrangemangen, om deltagandet av tredjepartsleverantörer av IKT-tjänster och om operativa delar. Finansiella entiteter ska också underrätta de behöriga myndigheterna om sitt deltagande i arrangemang för informationsutbyte.

Behöriga myndigheter

I kapitel VII i förordningen finns bestämmelser om behöriga myndigheter, som enligt artikel 46 ska säkerställa efterlevnaden av förordningen i enlighet med de befogenheter som tilldelats genom respektive rättsakt.

De europeiska tillsynsmyndigheterna och de behöriga myndigheterna får delta i verksamheten i den samarbetsgrupp som inrättats genom artikel 14 i NIS 2-direktivet i frågor som rör deras tillsynsverksamhet i samband med finansiella entiteter. De behöriga myndigheterna får när så är lämpligt samråda och utbyta information med den gemensamma kontaktpunkten och de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS 2-direktivet. De behöriga

myndigheterna kan också annars ingå samarbetsarrangemang med myndigheter i enlighet med det direktivet, och de ska ha ett nära samarbete sinsemellan och i tillämpliga fall med den ledande tillsynsmyndigheten.

I artikel 50 finns bestämmelser om administrativa sanktioner och avhjälpande åtgärder som behövs för att säkerställa att bestämmelserna följs, vilket förutsätter kompletterande nationell lagstiftning av medlemsstaterna. Utgångspunkten är att de behöriga myndigheterna ska ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen. I detta syfte ska medlemsstaterna fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen och säkerställa att de genomförs effektivt, dock utan att det påverkar medlemsstaternas rätt att besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt. Medlemsstaterna ska också ge behöriga myndigheter befogenhet att tillämpa åtminstone sådana sanktioner som anges närmare i artikel 50.4 a–e samt befogenhet att tillämpa administrativa sanktioner och avhjälpande åtgärder på medlemmar i ledningsorganet och på andra personer som enligt nationell rätt är ansvariga för överträdelsen. Alla beslut om att ålägga dessa administrativa sanktioner eller åtgärder ska vara vederbörligen motiverade och kunna överklagas. De behöriga myndigheterna ska utöva sina befogenheter att ålägga de administrativa sanktioner och avhjälpande åtgärder som avses i artikel 50 i enlighet med sina nationella rättsliga ramar.

Medlemsstaterna ska underrätta kommissionen, Esma, EBA och Eiopa om de lagar och andra författningar som genomför kapitel VII, inbegripet alla relevanta straffrättsliga bestämmelser senast den 17 januari 2025. De ska också ska utan onödigt dröjsmål underrätta kommissionen, Esma, EBA och Eiopa om eventuella ändringar av dessa.

Förordningens förhållande till NIS 2- och CER-direktiven

I NIS 2-direktivet fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Direktivet fastställer i detta syfte skyldigheter som ålägger medlemsstaterna att anta nationella strategier för cybersäkerhet och att utse eller inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser, gemensamma kontaktpunkter för cybersäkerhet och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter), riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilaga I eller II till direktivet samt för entiteter som identifieras som kritiska entiteter enligt CER-direktivet, regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet samt skyldigheter för medlemsstaterna när det gäller tillsyn och efterlevnadskontroll. NIS 2-direktivets innehåll beskrivs i större detalj i regeringens proposition om det nationella genomförandet av direktivet (RP –/2024 rd).

De högkritiska sektorerna enligt NIS 2-direktivet inkluderar bankverksamhet och finansmarknadsinfrastruktur, som under förutsättningarna enligt artikel 2 i direktivet omfattar tre typer av finansiella entiteter: kreditinstitut, operatörer av handelsplatser samt centrala motparter. EU:s DORA-förordning är speciallagstiftning (*lex specialis*) i förhållande till NIS 2-direktivet. Därför bör medlemsstaterna inte tillämpa NIS 2-direktivets bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet och om tillsyn och efterlevnadskontroll på finansiella entiteter som omfattas av EU:s DORA-förordning. Enligt skäl 16 i ingressen till förordningen är det samtidigt mycket viktigt att upprätthålla en stark koppling mellan finanssektorn och unionens övergripande ram för cybersäkerhet, för att säkerställa överensstämmelse med de strategier för cybersäkerhet som antagits av

medlemsstaterna och göra det möjligt för finansiella tillsynsmyndigheter att få kännedom om cyberincidenter som påverkar andra sektorer som omfattas av det direktivet. För att möjliggöra sektorsövergripande lärande och effektivt ta vara på erfarenheter från andra sektorer när det gäller att hantera cyberhot bör de finansiella entiteter som avses i NIS 2-direktivet enligt skäl 18 i förordningens ingress fortsätta att ingå i ”ekosystemet” i det direktivet (t.ex. samarbetsgrupp samt nätverket av entiteter för hantering av it-säkerhetsincidenter (CSIRT-enheter)). De europeiska tillsynsmyndigheterna och de nationella behöriga myndigheterna bör kunna delta i de strategiska politiska diskussionerna och det tekniska arbetet i samarbetsgruppen enligt det direktivet och kunna utbyta information och samarbeta ytterligare med de gemensamma kontaktpunkter som har utsetts eller inrättats i enlighet med det direktivet. I skäl 28 i ingressen till NIS 2-direktivet anges dessutom att de behöriga myndigheterna enligt EU:s DORA-förordning bör översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv. Detta kan ske genom att ge omedelbar tillgång till incidentanmälningar, och vidarebefordra dem antingen direkt eller genom en gemensam kontaktpunkt. Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet. I kommissionens meddelande om tillämpningen av artikel 4.1 och 4.2 i NIS 2-direktivet (2023/C 328/02) anges dessutom att NIS 2-direktivets artikel 9 om ramar för hantering av cybersäkerhetskriser och artikel 16 om det europeiska kontaktnätverket för cyberkriser EU-CyCLONe bör tillämpas i sin helhet på sektorer även om det finns sektorsspecifika unionsrättsakter.

I CER-direktivet fastställs skyldigheter för medlemsstaterna att vidta särskilda åtgärder som syftar till att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet inom tillämpningsområdet för artikel 114 i fördraget om Europeiska unionens funktionssätt tillhandahålls på ett obehindrat sätt på den inre marknaden, särskilt skyldigheter för att identifiera kritiska entiteter samt för att stödja kritiska entiteter i uppfyllandet av de skyldigheter som åläggs dem. I direktivet fastställs också skyldigheter för kritiska entiteter som syftar till att stärka deras motståndskraft och förmåga att tillhandahålla tjänster på den inre marknaden. Där fastställs regler om tillsyn av kritiska entiteter, om efterlevnadskontroll, för identifiering av kritiska entiteter av särskild europeisk betydelse samt om rådgivande uppdrag för att bedöma de åtgärder som sådana entiteter har infört för att uppfylla sina skyldigheter enligt kapitel III. Det inrättas gemensamma förfaranden för samarbete och rapportering om tillämpningen av detta direktiv samt fastställs åtgärder i syfte att uppnå en hög grad av motståndskraft för kritiska entiteter, för att säkerställa tillhandahållande av samhällsviktiga tjänster i unionen och förbättra den inre marknadens funktionssätt. CER-direktivets innehåll beskrivs i större detalj i regeringens proposition om det nationella genomförandet av direktivet (RP –/2024 rd).

Sektorerna enligt CER-direktivet inkluderar bankverksamhet och finansmarknadsinfrastruktur, i den mån aktörerna identifierats som kritiska enligt artikel 6 i direktivet och företräder tre typer av finansiella entiteter: kreditinstitut, operatörer av handelsplatser samt centrala motparter. I skäl 21 i ingressen till CER-direktivet anges att eftersom de finansiella entiteternas motståndskraft omfattas på ett heltäckande sätt av unionsrätten om finansiella tjänster bör artikel 11 och kapitlen III, IV och VI inte vara tillämpliga på dessa entiteter, för att undvika dubbelarbete och en onödig administrativ börda. Med tanke på hur viktiga de tjänster som tillhandahålls av entiteter i finanssektorn är för kritiska entiteter som tillhör alla andra sektorer, bör medlemsstaterna dock, med utgångspunkt i de kriterier och enligt det förfarande som föreskrivs i direktivet, identifiera entiteter i finanssektorn som kritiska entiteter. Följaktligen bör strategierna, medlemsstaternas riskbedömningar och de stödåtgärder som anges i kapitel II i direktivet vara tillämpliga. Medlemsstaterna bör ha rätt att anta eller behålla bestämmelser i

nationell rätt för att uppnå en högre grad av motståndskraft för dessa kritiska entiteter, förutsatt att dessa bestämmelser är förenliga med tillämplig unionsrätt.

DORA-ändringsdirektivet

I DORA-ändringsdirektivet finns bestämmelser om ändringar i flera av Europaparlamentets och rådets direktiv som gäller finansiella entiteter och som innehåller reglering om krav i fråga om IKT-riskhantering inom finanssektorn. Dessa är direktiv 2009/65/EG om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag) (nedan *fondföretagsdirektivet*), direktiv 2009/138/EG om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (nedan *Solvens II-direktivet*), direktiv 2011/61/EU 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 (nedan *AIFM-direktivet*), direktiv 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG (nedan *kreditinstitutsdirektivet*), direktiv 2014/59/EU om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt förordningarna (EU) nr 1093/2010 och (EU) nr 648/2012 (nedan *resolutionsdirektivet*), direktiv 2014/65/EU om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (nedan *MiFID II-direktivet*), direktiv (EU) 2015/2366 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 (nedan *betaltjänstdirektivet*) samt direktiv (EU) 2016/2341 om verksamhet i och tillsyn över tjänstepensionsinstitut (nedan *IORP II-direktivet*)

Ändringarna syftar till att säkerställa direktivens konsekvens med EU:s DORA-förordning. Enligt skäl 3 i ingressen till DORA-ändringsdirektivet är ändringarna nödvändiga för att bringa rättslig klarhet och enhetlighet i fråga om hur de finansiella entiteter som auktoriseras och övervakas i enlighet med dessa direktiv ska tillämpa olika krav på digital operativ motståndskraft som är nödvändiga för att de ska kunna bedriva sin verksamhet och tillhandahålla tjänster. Finansiella entiteter ska som en del av sin interna styrning och sina riskhanteringsförfaranden förvalta nätverks- och informationssystem i enlighet med EU:s DORA-förordning. Ändringarnas exakta innehåll varierar beroende på hur de olika direktiven reglerar organiseringen av verksamheten, riskhanteringen och kraven för motståndskraften och säkerställandet av verksamhetens kontinuitet.

Direktivet innehåller också vissa andra ändringar. Tillämpningsområdet för översyns- och utvärderingsprocessen enligt artikel 97 i kreditinstitutsdirektivet har ändrats så att det uttryckligen hänvisar till de krav som fastställs i EU:s DORA-förordning och omfattar särskilt risker som framkommit vid test av digitala operativ motståndskraft som kreditinstituten genomfört i enlighet med den förordningen. Genom DORA-ändringsdirektivet har också en bestämmelse fogats till kreditinstitutsdirektivet enligt vilken en behörig myndighet ska ha rätt att kräva all information den behöver för att kunna utföra sina uppgifter också av tredjepartsleverantörer av IKT-tjänster. Genom ändringarna i resolutionsdirektivet beaktas den digitala operativa motståndskraften och EU:s DORA-förordning i kraven på innehållet i kreditinstitutens och värdepappersföretagens återhämtnings- och resolutionsplaner samt i de krav som gäller bedömning av möjligheterna till resolution och omstrukturering.

Enligt skäl 9 i ingressen till direktivet har ytterligare IKT-krav i många fall redan fastställts i delegerade akter och genomförandeakter, antagna utifrån förslag till tekniska tillsynsstandarder och tekniska standarder för genomförande vilka utarbetats av den behöriga europeiska tillsynsmyndigheten. Eftersom bestämmelserna i EU:s DORA-förordning hädanefter utgör den rättsliga ramen för IKT-risk för finanssektorn ändras vissa befogenheter att anta delegerade akter och genomförandeakter i Solvens II-direktivet, AIFM-direktivet och MiFID II-direktivet för att utesluta IKT-riskbestämmelserna från tillämpningsområdet för dessa befogenheter.

Medlemsstaterna ska enligt artikel 9 i DORA-ändringsdirektivet senast den 17 januari 2025 anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Medlemsstaterna ska tillämpa dessa bestämmelser från och med samma datum.

3 Nuläge och bedömning av nuläget

3.1 Lagen om Finansinspektionen

Bestämmelser om Finansinspektionens uppgifter finns i 3 § i lagen om Finansinspektionen (878/2008). Finansinspektionen ska enligt 1 mom. utöva tillsyn över finansmarknadsaktörernas verksamhet enligt vad som föreskrivs i den lagen och i andra lagar. Dessutom främjar Finansinspektionen goda förfaranden på finansmarknaden och allmänhetens kunskaper om finansmarknaden.

I 2 och 3 mom. finns bestämmelser om Finansinspektionens särskilda uppgiftsområden. Enligt förarbetena till lagen (RP 66/2008 rd, s. 84) är syftet med paragrafen att beskriva Finansinspektionens viktigaste uppgifter. Frågan om i vilken utsträckning Finansinspektionen ska sköta respektive uppgiftsområde och hur den ska fördela sina resurser mellan uppgiftsområdena blir beroende av de närmare målsättningar och tyngdpunktsområden som Finansinspektionens direktion bestämmer för verksamheten. I 2 mom. finns bestämmelser om de av Finansinspektionens uppgifter vilkas närmare innehåll bestäms beroende på vad som föreskrivs i annan lag. I 3 mom. föreskrivs om mer allmänna uppgifter för vilka Finansinspektionen har befogenheter enbart med stöd av denna paragraf.

Till Finansinspektionens uppgifter hör bland annat enligt 2 mom. 2 punkten att övervaka att finansmarknadsaktörerna iakttar de på dem tillämpliga bestämmelserna om finansmarknaden och med stöd av dem utfärdade föreskrifter, villkoren i sina verksamhetstillstånd och stadgarna som gäller deras verksamhet, samt enligt 3 mom. 6 punkten att delta i det nationella samarbetet mellan myndigheter och enligt 3 mom. 7 punkten att delta i det samarbete inom Europeiska unionen som sker inom ramen för det europeiska system för finansiell tillsyn som avses i 3 a § och i annat internationellt myndighetssamarbete.

Bestämmelser om Finansinspektionens tillsynsbefogenheter finns i 3 kap. i lagen om Finansinspektionen. Enligt 18 § i den lagen ska tillsynsobjekt och andra finansmarknadsaktörer utan hinder av sekretessbestämmelserna och utan obefogat dröjsmål till Finansinspektionen lämna de för utförandet av dess lagstadgade uppdrag relevanta uppgifter och redogörelser som den ber om. Motsvarande skyldighet har den som i ett tillsynsobjekt eller en annan finansmarknadsaktör har bestämmande inflytande enligt 1 kap. 5 § i bokföringslagen (1336/1997) och den som tillsynsobjektet eller någon annan finansmarknadsaktör har bestämmande inflytande i. Detta gäller också företag som i egenskap av ombud för tillsynsobjekt eller andra finansmarknadsaktörer, i egenskap av anknutet ombud enligt 7 kap. 6 § i lagen om investeringstjänster eller annars på uppdrag av tillsynsobjekt eller andra finansmarknadsaktörer sköter uppgifter i anslutning till dessas affärsverksamhet, bokföring, datasystem, riskhantering eller interna kontroll. Rätten att få uppgifter omfattar med stöd av 19

§ också uppgifter av tillsynsobjekts och andra finansmarknadsaktörers revisorer som Finansinspektionen behöver för att fullgöra sitt lagstadgade tillsynsuppdrag, samt för en viss tillsynsåtgärd relevanta uppgifter av andra om de av grundad anledning kan antas vara i besittning av information som är nödvändig för tillsynen.

Enligt 22 § har Finansinspektionen rätt att vid behov kalla in och höra representanter för eller anställda hos juridiska personer som avses i 18, 19 och 21 § eller fysiska personer som avses i de paragraferna. Då tillämpas förvaltningslagens (434/2003) bestämmelser om muntlig behandling. Den som underlåter att följa en kallelse kan inte föreläggas vite enligt 33 a § eller påföras en administrativ påföljd enligt 4 kap.

Enligt 24 § 1 mom. har Finansinspektionen trots sekretessbestämmelserna rätt att på tillsynsobjekts och andra finansmarknadsaktörers verksamhetsställen granska handlingar, upptagningar av telefonsamtal och elektronisk kommunikation, andra datatrafikuppgifter samt datasystem som gäller dessas verksamhet och förvaltning, i den utsträckning som behövs för att den ska kunna fullgöra sitt lagstadgade tillsynsuppdrag. Finansinspektionen har rätt att av tillsynsobjekt och andra finansmarknadsaktörer avgiftsfritt få behövliga kopior av sådana handlingar och andra upptagningar och datatrafikuppgifter som avses i denna paragraf. Vad som i 1 mom. föreskrivs om tillsynsobjekt och andra finansmarknadsaktörer gäller enligt 2 mom. också företag som i egenskap av ombud för tillsynsobjekt eller andra finansmarknadsaktörer, i egenskap av anknutet ombud enligt 7 kap. 6 § i lagen om investeringstjänster eller annars på uppdrag av tillsynsobjekt eller andra finansmarknadsaktörer sköter uppgifter i anslutning till dessas affärsverksamhet, bokföring, datasystem, riskhantering eller interna kontroll. Enligt 3 mom. har Finansinspektionen dessutom utan hinder av sekretessbestämmelserna rätt att av personer och företag som avses i lagens 19, 21 och 23 § för granskning få handlingar och upptagningar som innehåller information av det slag som avses i nämnda paragraf.

Med stöd av 25 b § har Finansinspektionen rätt att på begäran få handräckning av polisen vid utförandet av uppdrag.

I 33 § föreskrivs om verkställighetsförbud och rättelseuppmaning. Enligt 1 mom. kan Finansinspektionen förbjuda verkställigheten av tillsynsobjekts och andra finansmarknadsaktörers beslut och av tillsynsobjekts och andra finansmarknadsaktörers planerade åtgärder, om beslutet eller åtgärden strider mot sådana bestämmelser om finansmarknaden som ska tillämpas på tillsynsobjekt och andra finansmarknadsaktörer eller mot bestämmelser som utfärdats med stöd av de bestämmelserna, mot tillståndsvillkor eller mot föreskrifter som gäller tillsynsobjekt eller andra finansmarknadsaktörers verksamhet. Om ett tillsynsobjekt eller någon annan finansmarknadsaktör har verkställt ett beslut enligt 1 mom. eller genomfört sådana andra åtgärder som avses i 1 mom. kan Finansinspektionen enligt 2 mom. ålägga tillsynsobjektet eller en annan finansmarknadsaktör att vidta åtgärder för att verkställa beslutet, återkalla åtgärden eller vidta rättelseåtgärder. Finansinspektionen ska för tillsynsobjektet eller en annan finansmarknadsaktör reservera en skälig tid för att verkställa beslutet, återkalla åtgärden eller vidta rättelseåtgärder, om detta inte allvarligt äventyrar de mål för tillsynen över finansmarknaden som föreskrivs i 1 §. Enligt 3 mom. kan Finansinspektionen ålägga tillsynsobjekt och andra finansmarknadsaktörer att upphöra med ett förfarande och förbjuda upprepning av förfarandet, om det strider mot de bestämmelser, föreskrifter, tillståndsvillkor eller regler som avses i 1 mom. Finansinspektionen ska ge ett tillsynsobjekt eller en finansmarknadsaktör tillfälle att inom en skälig tid rätta sitt förfarande, om detta inte allvarligt äventyrar de mål för tillsynen över finansmarknaden som föreskrivs i 1 §. Enligt 5 mom. kan sådana förbud och rättelseuppmaningar som avses i paragrafen av särskilda skäl riktas också till tillsynsobjekts och andra finansmarknadsaktörers anställda eller till andra som handlar för dess räkning.

I 33 a § föreskrivs det om vite. Om ett tillsynsobjekt eller en annan finansmarknadsaktör försummar att i sin verksamhet följa bestämmelserna om finansmarknaden eller föreskrifter som har utfärdats med stöd av dem, ett verkställighetsförbud eller en rättelseuppmaning som Finansinspektionen har utfärdat med stöd av 33 § eller något annat förordnande eller förbud som Finansinspektionen har utfärdat med stöd av lag, villkoren i sitt verksamhetstillstånd eller stadgarna om sin verksamhet, kan Finansinspektionen vid vite ålägga tillsynsobjektet eller finansmarknadsaktören att fullgöra sin skyldighet, om försummelsen inte är obetydlig. Vite kan således av särskilda skäl föreläggas också anställda hos tillsynsobjekt eller andra finansmarknadsaktörer samt andra som handlar för deras räkning. Finansinspektionen kan vid vite ålägga den som avses i 18, 19, 21, 23 och 24 § att fullgöra sin skyldighet enligt de paragraferna, om försummelsen inte är obetydlig.

Enligt 34 § kan Finansinspektionen för en utredning som behövs för tillsynen över ett tillsynsobjekt eller en annan finansmarknadsaktör och som kräver särskild sakkunskap anlita en revisor eller en annan utomstående sakkunnig. Denne handlar under straffrättsligt tjänsteansvar och har de rättigheter som nämns i 18, 19, 23 och 24 § vid utförandet av sina offentligrättsliga förvaltningsuppgifter enligt denna lag.

I 4 kap. i lagen om Finansinspektionen finns bestämmelser om administrativa påföljder. Dessa påföljder är ordningsavgift enligt 38 §, offentlig varning enligt 39 § och påföljdsavgift enligt 40 §. I paragraferna om ordningsavgift och påföljdsavgift anges vilka bestämmelser som ska ha försummats eller brutits mot för att påföljden ska kunna påföras. Om gärningen eller försummelsen är särskilt klandervärd kan det enligt 38 § 4 mom. i stället för ordningsavgift påföras en påföljdsavgift.

Enligt 39 § ska Finansinspektionen meddela tillsynsobjekt och andra finansmarknadsaktörer offentlig varning om de uppsåtligen eller av oaktsamhet handlar i strid med andra bestämmelser om finansmarknaden än de som avses i 38 § 1 mom. eller 40 § 1 eller 2 mom. eller i strid med föreskrifter som utfärdats med stöd av de bestämmelserna, under förutsättning att ärendet bedömt som en helhet inte föranleder strängare åtgärder.

Enligt 40 § 3 mom. kan påföljdsavgift inte påföras en fysisk person för en gärning eller försummelse som enligt lag är straffbar. Finansinspektionen får dock påföra påföljdsavgift och avstå från att anmäla ärendet till förundersökningsmyndigheten, om gärningen eller försummelsen med hänsyn till dess menlighet, gärningsmannens skuld sådan den framgår av gärningen, den vinning som erhållits och övriga omständigheter i anslutning till gärningen eller försummelsen anses vara ringa bedömd som en helhet. Enligt 4 mom. kan påföljdsavgift, utöver eller i stället för en påföljdsavgift som påförs en juridisk person, påföras en sådan person i den juridiska personens ledning vars förpliktelser har åsidosatts genom en gärning eller försummelse som avses i denna paragraf. En förutsättning för att personen i fråga ska påföras påföljdsavgift är att denne på ett betydande sätt har bidragit till gärningen eller försummelsen.

I 41 § föreskrivs det om påförande av påföljdsavgift. Enligt 2 mom. ska påföljdsavgiftens belopp baseras på en samlad bedömning, på samma sätt som ordningsavgiften enligt 38 § 2 mom. Vid bedömningen ska hänsyn tas till förfarandets art, omfattning och varaktighet samt gärningsmannens ekonomiska ställning. Dessutom ska vid bedömningen beaktas den vinning som erhållits och den skada som orsakats genom förfarandet, om vinningen eller skadan kan bestämmas, gärningsmannens samarbete med Finansinspektionen för att utreda ärendet, åtgärder för att förhindra att överträdelsen upprepas, gärningsmannens övriga och tidigare överträdelser och försummelser i fråga om bestämmelserna om finansmarknaden och förfarandets eventuella konsekvenser för det finansiella systemets stabilitet.

Enligt 42 § 1 mom. kan Finansinspektionen avstå från att påföra ordningsavgift eller från att meddela offentlig varning, om 1) den som avses i 38 eller 39 § självmant har vidtagit tillräckliga korrigerande åtgärder omedelbart efter att ha upptäckt felet, utan dröjsmål har anmält felet till Finansinspektionen och det inte är fråga om allvarliga eller upprepade fel eller försummelser, 2) det felaktiga förfarandet kan anses vara obetydligt, eller 3) det annars måste anses vara uppenbart oskäligt att påföra ordningsavgift eller meddela offentlig varning. Enligt 2 mom. kan Finansinspektionen i stället för att påföra en påföljdsavgift meddela en offentlig varning på de grunder som föreskrivs i 1 mom. 2 och 3 punkten. Enligt 3 mom. kan ordningsavgift eller påföljdsavgift inte påföras en person som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som behandlas i domstol. Ordningsavgift eller påföljdsavgift kan inte heller påföras den som har dömts för samma gärning genom en lagakraftvunnen dom.

Enligt 43 § 1 mom. ska Finansinspektionen utan dröjsmål offentliggöra ordningsavgifter, offentliga varningar och påföljdsavgifter efter det att den person som är föremål för beslutet har informerats om detta. Av offentliggörandet ska framgå huruvida beslutet att påföra eller meddela påföljden har vunnit laga kraft, överträdelsens art och slag samt identiteten hos den person som är ansvarig för överträdelsen. Information om en påföljd ska finnas tillgänglig på Finansinspektionens webbplats i fem år. Under de förutsättningar som anges i 2 mom. kan Finansinspektionen skjuta upp offentliggörandet av beslutet om påföljd, offentliggöra beslutet om påföljd utan att ange namnet på den som ålagts en påföljd eller låta bli att offentliggöra ett beslut om påföljd, om det är oskäligt att namnet på den fysiska eller juridiska person som ålagts en påföljd offentliggörs eller om offentliggörandet av påföljden äventyrar stabiliteten på finansmarknaden eller en pågående myndighetsundersökning. Vad som i den paragrafen föreskrivs om offentliggörande av ordningsavgift, offentlig varning och påföljdsavgift tillämpas också på offentliggörande av sådana beslut som avses bland annat i 33 och 33 a § i lagen.

I kapitel 6 i lagen om Finansinspektionen finns bestämmelser om bland annat Finansinspektionens samarbete med utländska myndigheter och tillsynen över iakttagande av EU-rättsakter. Genom de gällande paragraferna 50 p § och 52 a § genomfördes Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (*direktivet om nät- och informationssäkerhet*).

Enligt 50 p § är Finansinspektionen behörig myndighet enligt artikel 8.1 i direktivet om nät- och informationssäkerhet när det gäller sektorerna 3 och 4 i bilaga II till direktivet.

Enligt 52 a § ska Finansinspektionen samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet. Finansinspektionen har för detta syfte rätt att trots bestämmelserna om sekretess lämna ut uppgifter till Transport- och kommunikationsverket. Genom paragrafen genomfördes artikel 10 i direktivet om nät- och informationssäkerhet i fråga om sektorerna 3 och 4 i bilaga II till direktivet. I artikel 10 i direktivet finns bestämmelser om myndighetssamarbete på nationell nivå. Om den behöriga myndigheten, den gemensamma kontaktpunkten och CSIRT-enheten i en och samma medlemsstat är separata, ska de samarbeta när det gäller fullgörandet av skyldigheterna enligt direktivet. Medlemsstaterna ska säkerställa att antingen de behöriga myndigheterna eller CSIRT-enheterna mottar incidentrapporter som lämnas in i enlighet med direktivet. Om en medlemsstat beslutar att CSIRT-enheterna inte ska motta rapporter ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till uppgifter om incidenter som rapporterats av leverantörer av samhällsviktiga tjänster enligt artikel 14.3 och 14.5 i direktivet. Medlemsstaterna ska säkerställa att de behöriga myndigheterna eller CSIRT-enheterna informerar de gemensamma kontaktpunkterna om incidentrapporter som lämnats in i enlighet med direktivet. Cybersäkerhetscentret vid Transport- och

kommunikationsverket är den gemensamma kontaktpunkt och CSIRT-enhet som avses i direktivet om nät- och informationssäkerhet.

Enligt 18 § 2 mom. i lagen om Finansinspektionen får Finansinspektionen meddela föreskrifter bland annat om vilka uppgifter om tillsynsobjekts interna kontroll och riskhantering som regelbundet ska lämnas till Finansinspektionen och om hur informationen ska lämnas. Finansinspektionen har meddelat föreskrifter och anvisningar om hantering av operativa risker i företag under tillsyn inom finanssektorn (Föreskrifter och anvisningar 8/2014), som trädde i kraft den 1 februari 2015.

Som en del av dessa föreskrifter och anvisningar meddelade Finansinspektionen föreskrifter om rapportering av uppgifter om internkontroll, riskhantering och störningar till Finansinspektionen, som trädde i kraft den 1 januari 2020. Tillsynsobjektet ska utan dröjsmål göra en första anmälan till Finansinspektionen om betydande störningar och fel i tjänster som tillhandahålls för kunderna och i betalnings- och IT-systemen omedelbart när de yppat sig. En betydande störning i betalningsförmedlingen eller vid kortbetalningar är till exempel en störning eller ett dröjsmål som gäller ett stort antal kunder. En betydande störning är också en störning eller avvikelse i nätverks- och informationssäkerheten samt en störning där kundinformation har hamnat i händerna på utomstående. Finansinspektionen ska omedelbart underrättas också om sådana störningar och fel som skadar eller äventyrar tillsynsobjektets förmåga att fortsätta sin verksamhet eller svara för sina åtaganden. Tillsynsobjektet ska lämna in en kompletterande anmälan till Finansinspektionen om de närmare detaljerna i störningen så snabbt som möjligt efter den första anmälan och en slutrapport efter att den egentliga orsaken till störningen har utretts. Anmälan ska lämnas åtminstone om följande kategorier av störningar: intrång i IT-system, uppgifter har avslöjats för utomstående, kränkning av informationssäkerheten, spridning av fientliga program i IT-systemet samt överbelastningsattack.

Finansinspektionen har också meddelat föreskrifter och anvisningar om upptagande av verksamhet och företagsstyrningssystem i liv- och skadeförsäkringsbolag (Föreskrifter och anvisningar 6/2015), som trädde i kraft den 1 januari 2016 och innehåller föreskrifter och anvisningar om ordnandet av datasystem och datasäkerhet som en del av hanteringen av operativa risker i liv- och skadeförsäkringsbolag samt om inlämnande av uppgifter till Finansinspektionen. Finansinspektionens föreskrifter för liv- och skadeförsäkringsbolag om anmälan om störningar och fel i verksamheten motsvarar huvudsakligen föreskrifterna för andra företag under tillsyn inom finanssektorn.

3.2 Ändringar som EU:s DORA-förordning förutsätter i Finansinspektionens tillsynsbefogenheter

EU:s DORA-förordning är direkt tillämplig rätt i Finland. De finansiella entiteter som omfattas av förordningens tillämpningsområde är därmed skyldiga att följa bestämmelserna i förordningen utan särskilda nationella genomförandeåtgärder. Finansinspektionen är i Finland den behöriga myndighet som avses i artikel 46 i EU:s DORA-förordning. Finansinspektionens uppgift är att övervaka att finansmarknadsaktörerna iakttar de på dem tillämpliga bestämmelserna om finansmarknaden, vilket i fortsättningen också inkluderar EU:s DORA-förordning. Artikel 50.1 i förordningen förutsätter att de behöriga myndigheterna ska ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen. Bestämmelserna om den behöriga myndighetens befogenheter finns huvudsakligen i den nationella lagstiftningen, och till den delen förutsätter förordningen nationella lagstiftningsåtgärder.

Enligt artikel 50.2 a i EU:s DORA-förordning ska befogenheterna omfatta befogenheten att få tillgång till alla dokument eller uppgifter som enligt den behöriga myndigheten är relevanta för fullgörandet av dess uppgifter och få eller ta en kopia av dem. Enligt punkt 2 led b i artikeln ska den behöriga myndigheten ha befogenheter att utföra kontroller eller inspektioner på plats, som ska omfatta men inte vara begränsade till att kalla till sig företrädare för finansiella entiteter och be dem om muntliga eller skriftliga förklaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren och höra vilken annan fysisk eller juridisk person som helst som går med på att höras i syfte att samla in information om föremålet för utredningen. Dessa befogenheter ingår i 18, 19, 22 och 24 § i lagen om Finansinspektionen.

Enligt artikel 50.2 c i EU:s DORA-förordning ska den behöriga myndigheten ha befogenheter att kräva korrigerande och avhjälpande åtgärder vid överträdelser av kraven i förordningen. Enligt artikel 50.3 ska medlemsstaterna utan att det påverkar deras rätt att ålägga straffrättsliga påföljder i enlighet med artikel 52 fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen och säkerställa att de genomförs effektivt. Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande.

De krav som gäller administrativa sanktioner och avhjälpande åtgärder preciseras i artikel 50.4 i EU:s DORA-förordning. Enligt led a och b ska medlemsstaterna ge behöriga myndigheter befogenhet att vid överträdelser av förordningen utfärda ett föreläggande enligt vilket det krävs att den fysiska eller juridiska personen upphör med det agerande som strider mot förordningen och inte upprepar detta agerande, samt kräva att varje praxis eller beteende som den behöriga myndigheten anser strider mot bestämmelserna i förordningen tillfälligt eller permanent upphör och förhindra en upprepning av denna praxis eller detta beteende. Dessa befogenheter ingår i 33 § i lagen om Finansinspektionen.

Enligt artikel 50.4 c i EU:s DORA-förordning ska de behöriga myndigheterna ges befogenheter att vidta vilken typ av åtgärd som helst, även av ekonomisk art, för att säkerställa att finansiella entiteter fortsätter att uppfylla sina rättsliga krav. I fråga om vite ingår dessa befogenheter i 33 a § i lagen om Finansinspektionen. Även bestämmelserna om administrativa påföljder i lagens 4 kap. är relevanta i detta avseende. I lagens bestämmelser om ordningsavgift och påföljdsavgift anges vilka bestämmelser som ska ha försummats eller brutits mot för att påföljden ska kunna påföras. Dessa bestämmelser bör kompletteras så att en påföljd kan påföras den som försummar eller bryter mot de relevanta bestämmelserna i EU:s DORA-förordning. Administrativa påföljder enligt den lagen gör det möjligt att snabbt och effektivt ingripa i förfaranden som strider mot lagstiftningen, vilket effektiviserar tillsynen över finansiella entiteter. Bestämmelserna om administrativa påföljder tryggar också genom sin allmänna förebyggande effekt att lagens krav följs.

Enligt artikel 50.4 d i EU:s DORA-förordning ska de behöriga myndigheterna ha befogenhet att kräva tillgång till, i den mån det är tillåtet enligt nationell rätt, befintliga uppgifter om datatrafik som innehas av en teleoperatör om det föreligger en rimlig misstanke om överträdelse av förordningen och om dessa uppgifter kan vara relevanta för en utredning av överträdelser av förordningen. I den nationella lagstiftningen har Finansinspektionen inte getts rätt att kräva tillgång till uppgifter om datatrafik som innehas av en teleoperatör. Frågan bedömdes vid behandlingen av lagförslagen i anslutning till EU:s marknadsmissbruksförordning (EU) nr 596/2014 (se RP 65/2016 rd, s. 26). Marknadsmissbruksförordningen innehåller en motsvarande bestämmelse som EU:s DORA-förordning om befogenhet att kräva uppgifter om datatrafik som innehas av en teleoperatör i den mån det är tillåtet enligt nationell rätt. I Finland har endast polisen rätt att få teleövervakningsuppgifter i enlighet med bestämmelserna i tvångsmedelslagen (806/2011), och vid bland annat misstankar om grovt missbruk av

insiderinformation eller grov marknadsmanipulation kan polisen få domstolens tillstånd till teleövervakningsuppgifter. Det är inte befogat att ändra detta förhållningssätt utan en ingående bedömning av huruvida Finansinspektionens nuvarande undersökningsbefogenheter är tillräckliga. Valet att avstå från nationella bestämmelser om en sådan befogenhet måste betraktas som en möjlighet också enligt EU:s DORA-förordning.

Enligt artikel 50.4 e i förordningen ska de behöriga myndigheterna ges befogenheter att utfärda offentliga meddelanden, inbegripet offentliga uttalanden, med uppgift om den fysiska eller juridiska personens identitet och överträdelsens art. Dessa befogenheter ingår i 43 § i lagen om Finansinspektionen. Det som föreskrivs i den paragrafen om att offentliggöra ordningsavgifter, offentliga varningar och påföljdsavgifter tillämpas också på offentliggörande av beslut om verkställighetsförbud och rättelseuppmaning enligt 33 § och vite enligt 33 a § i den lagen. I artikel 54 i förordningen finns dessutom särskilda direkt tillämpliga bestämmelser om offentliggörande av administrativa sanktioner. De behöriga myndigheterna ska utan onödigt dröjsmål på sina officiella webbplatser offentliggöra alla beslut om att ålägga en administrativ sanktion som inte kan överklagas efter det att sanktionens adressat har underrättats om beslutet. Artikeln innehåller dessutom undantag från skyldigheten att offentliggöra besluten samt andra preciserande bestämmelser. Finansinspektionen ska beakta de bestämmelserna i sin verksamhet vid sidan av den nationella lagstiftningen. Det är motiverat att ta in en informativ hänvisningsbestämmelse om detta i lagen om Finansinspektionen.

Om punkt 2 c och punkt 4 är tillämpliga på juridiska personer ska medlemsstaterna enligt artikel 50.5 i EU:s DORA-förordning ge de behöriga myndigheterna befogenhet att tillämpa administrativa sanktioner och avhjälpande åtgärder, med förbehåll för de villkor som föreskrivs i nationell rätt, på medlemmar i ledningsorganet och på andra personer som enligt nationell rätt är ansvariga för överträdelsen. Bestämmelser om detta ingår i 33 § 5 mom. och 40 § 4 mom. i lagen om Finansinspektionen.

Enligt artikel 50.6 i förordningen ska medlemsstaterna säkerställa att alla beslut om att ålägga administrativa sanktioner eller avhjälpande åtgärder enligt punkt 2 c är vederbörligen motiverade och kan överklagas. Bestämmelser om överklagande av Finansinspektionens beslut finns i 73 § i lagen om Finansinspektionen. Bestämmelser om förvaltningsförfarandet finns i förvaltningslagen.

De behöriga myndigheterna ska enligt artikel 51.2 i EU:s DORA-förordning, när de fastställer typen av och nivån på en administrativ sanktion eller avhjälpande åtgärd som ska åläggas enligt artikel 50, ta hänsyn till i vilken utsträckning överträdelsen är avsiktlig eller beror på försummelse och till alla andra relevanta omständigheter, bland annat följande, när så är lämpligt:
a) överträdelsens väsentlighet, svårighetsgrad och varaktighet,
b) graden av ansvar hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen,
c) den finansiella styrkan hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen,
d) omfattningen av de vinster som erhållits eller av förluster som undvikits av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen, i den mån de kan bestämmas,
e) förluster för tredje parter orsakade av överträdelsen, i den mån de kan fastställas,
f) viljan hos den ansvariga fysiska eller juridiska personen att samarbeta med den behöriga myndigheten, utan att det påverkar behovet av att säkerställa återföring av den vinst som den fysiska eller juridiska personen gjort eller de förluster som denne undvikit,
g) tidigare överträdelser av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen.

Bestämmelser om faktorer som ska beaktas när beloppet på ordningsavgift och påföljdsavgift bestäms finns i 38 § 2 mom. och 41 § 2 mom. i lagen om Finansinspektionen. Beloppet på ordningsavgiften eller påföljdsavgiften baseras på en samlad bedömning. När en påföljd som påförs för försummelse av eller brott mot skyldigheterna enligt EU:s DORA-förordning fastställs ska åtminstone alla de omständigheter som nämns i förordningens artikel 51.2 och alla andra relevanta omständigheter beaktas. Punkten gäller åläggande av såväl administrativa sanktioner som andra avhjälpande åtgärder. Finansinspektionen ska i sin verksamhet beakta dessa direkt tillämpliga bestämmelser vid sidan av den nationella lagstiftningen. Det är motiverat att ta in en informativ hänvisningsbestämmelse om detta i lagen om Finansinspektionen.

Enligt artikel 52 i EU:s DORA-förordning får medlemsstaterna besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt. Det är alltså upp till medlemsstaten att avgöra om överträdelser av förordningen till någon del ska göras straffrättsligt straffbara.

Utifrån det som anförs ovan kan man konstatera att tillsynsbefogenheterna enligt 3 kap. i lagen om Finansinspektionen ger Finansinspektionen de omfattande tillsyns- och utredningsbefogenheter som förutsätts i artikel 50 i EU:s DORA-förordning för att se till att förordningen följs, och därmed behöver inte dessa bestämmelser ändras med anledning av förordningen. Däremot konstateras det ovan att kompletterande nationell reglering behövs när det gäller administrativa påföljder enligt 4 kap. i lagen för att säkerställa effektiva, proportionella och avskräckande administrativa påföljder på det sätt som EU:s DORA-förordning förutsätter.

Till Finansinspektionens uppgifter hör, som en del av tillsynen över att skyldigheterna enligt EU:s DORA-förordning fullgörs, att övervaka finansiella entiteters sunda hantering av IKT-tredjepartsrisker. När finansiella entiteter i sin verksamhet stöder sig på tredjepartsleverantörer av IKT-tjänster förutsätter en övergripande bedömning av IKT-risken också insyn i tjänsteleverantörens verksamhet, även om den finansiella entiteten fortfarande har ansvaret för att skyldigheterna enligt förordningen fullgörs. Därmed omfattar tillsynen indirekt också verksamheten hos de tredjepartsleverantörer av IKT-tjänster som avses i förordningen och deras egna IKT-riskhanteringsförfaranden. I artikel 30 i förordningen föreskrivs det dessutom om faktorer som finansiella entiteter och tredjepartsleverantörer av IKT-tjänster ska ta i beaktande när de ingår avtal om dessa tjänster. Därför bör man i lagen göra de ändringar som behövs för att Finansinspektionens tillsynsbefogenheter ska omfatta tredjepartsleverantörer av IKT-tjänster. Detta behövs också eftersom en behörig myndighet enligt DORA-ändringsdirektivet ska ha rätt att kräva all information den behöver för att kunna utföra sina uppgifter också av tredjepartsleverantörer av IKT-tjänster. Av detta följer också att en behörig myndighet i enlighet med artikel 65.3 i kreditinstitutsdirektivet ska ha rätt att genomföra alla nödvändiga utredningar av tredjepartsleverantörer av IKT-tjänster och befogenhet att genomföra alla nödvändiga kontroller i tjänsteleverantörens företagslokaler.

3.3 Andra ändringar som EU:s DORA-förordning förutsätter i lagen om Finansinspektionen

Enligt artikel 19.6 i EU:s DORA-förordning ska den behöriga myndigheten efter mottagandet av den första anmälan om en allvarlig IKT-relaterad incident och av varje rapport som avses i artikelns punkt 4 skyndsamt lämna närmare uppgifter om incidenten, i tillämpliga fall på grundval av deras respektive behörigheter, till EBA, Esma eller Eiopa, vid behov till ECB, till de behöriga myndigheter, de gemensamma kontaktpunkter eller de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS 2-direktivet, till resolutionsmyndigheterna och till andra relevanta offentliga myndigheter enligt nationell rätt. Finansiella entiteter får dessutom på

frivillig basis rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att hotet är relevant för det finansiella systemet, tjänsteanvändarna eller kunderna. Den relevanta behöriga myndigheten får med stöd av punkt 2 lämna sådan information till de ovannämnda myndigheterna. Därmed har Finansinspektionen direkt med stöd av artikel 19 i EU:s DORA-förordning rätt att trots sekretessbestämmelserna lämna i artikeln avsedd information om allvarliga IKT-relaterade incidenter och betydande cyberhot till dessa myndigheter. I artikel 55 i EU:s DORA-förordning finns bestämmelser om tystnadsplikt som omfattar all konfidentiell information som är föremål för mottagande, utbyte eller förmedling enligt förordningen. Information som avser affärs- eller driftsförhållanden och andra ekonomiska eller personliga förhållanden ska anses vara konfidentiell och omfattas av tystnadsplikt. Eftersom förordningen är direkt tillämplig rätt behöver inga ändringar göras i den nationella lagstiftningen när det gäller lämnande av denna information. För att åstadkomma en uppdaterad lägesbild av cybersäkerheten och främja den sektorsövergripande samordningen är det viktigt att Finansinspektionen utan obefogat dröjsmål förmedlar mottagna störningsanmälningar till Transport- och kommunikationsverkets Cybersäkerhetscenter och andra viktiga myndigheter. Andra viktiga aktörer är åtminstone parterna i samarbetsdokumentet för krishantering på finansmarknaden, som förutom Finansinspektionen är finansministeriet, social- och hälsovårdsministeriet, Finlands Bank och Verket för finansiell stabilitet.

Bestämmelsen i 18 § 2 mom. i lagen om Finansinspektionen, med stöd av vilken Finansinspektionen får meddela föreskrifter om att vissa uppgifter ska lämnas och hur de ska lämnas, behöver inte ändras med anledning av EU:s DORA-förordning. I de föreskrifter som meddelas med stöd av den bestämmelsen måste Finansinspektionen dock beakta att finansiella entiteter direkt med stöd av artikel 19 i EU:s DORA-förordning är skyldiga att rapportera om allvarliga IKT-relaterade incidenter. Föreskrifterna ska inte innehålla rapporteringsskyldigheter som överlappar med förordningen. Samtidigt utgör inte EU:s DORA-förordning något hinder för att meddela andra föreskrifter om rapportering med stöd av 18 § 2 mom. eller andra tillämpliga nationella bestämmelser. Enligt artikel 17.2 i förordningen ska finansiella entiteter registrera alla IKT-relaterade incidenter och betydande cyberhot. Det kan vara motiverat att i bestämmelserna förutsätta att finansiella entiteter eller vissa typer av finansiella entiteter rapporterar också andra än allvarliga incidenter till Finansinspektionen, särskilt om det allmänna cybersäkerhetsläget och utarbetandet av en uppdaterad lägesbild förutsätter det.

Enligt artikel 26.9 i EU:s DORA-förordning får medlemsstaterna utse en enda offentlig myndighet inom finanssektorn som ska ansvara för frågor som rör hotbildsstyrd penetrationstestning inom den finansiella sektorn på nationell nivå och ska ge myndigheten alla befogenheter och uppgifter i detta syfte. Om det inte har utsetts någon myndighet, och utan att det påverkar befogenheten att välja ut vilka finansiella entiteter som är skyldiga att utföra hotbildsstyrd penetrationstestning, får en behörig myndighet med stöd av punkt 10 delegera vissa eller alla av de uppgifter som avses i artikel 26 och 27 i EU:s DORA-förordning till en annan nationell myndighet inom den finansiella sektorn. Till den delen förutsätter alltså förordningen ingen nationell reglering, och när sådan reglering saknas får Finansinspektionen delegera uppgifter direkt med stöd av EU:s DORA-förordning. I praktiken kan den andra nationella myndighet inom den finansiella sektorn som avses i förordningen vara Finlands Bank, som för närvarande ansvarar för TIBER-FI-modellen. TIBER-FI är ett ramverk som tagits fram för Finlands finansiella aktörer för att säkra driftssäkerheten i finanssektorns kritiska funktioner mot riktade cyberattacker. Det baserar sig på Europeiska centralbankens modell TIBER-EU för utveckling av cybersäkerheten inom finanssektorn. TIBER-EU, som baseras på aktuell information om cybersäkerhetshot, är en systematisk, kontrollerad modell för att utföra Red Team-datasäkerhetstestning. Med stöd av EU:s DORA-förordning identifierar Finansinspektionen de finansiella entiteter som förutsätts utföra hotbildsstyrd penetrationstestning. Som en del av tillsynen över att EU:s DORA-förordning följs bör man

säkerställa att de finansiella entiteterna utför testningen enligt kraven. Myndigheterna ska också förse finansiella entiteter med ett intyg som bekräftar att testet genomfördes i enlighet med kraven, vilket ska framgå av den dokumentation som lämnats till myndigheterna. Det faller sig naturligt att sådana uppgifter ingår i tillsynsmyndighetens, det vill säga Finansinspektionens, ansvarsområde medan Finlands Bank även i fortsättningen ansvarar för att förvalta den modell som används för testningen. Uppgifterna enligt artiklarna 26 och 27 i förordningen inbegriper också utövning av offentlig makt, och därför måste myndighetsuppgifterna och de relaterade befogenheterna anges tydligt i lagstiftningen. Därmed är det motiverat att utse Finansinspektionen till den myndighet som avses i artikel 26.9 i EU:s DORA-förordning.

3.4 Andra behov av ändringar i lagen om Finansinspektionen

Direktivet om nät- och informationssäkerhet upphävdes genom NIS 2-direktivet. Därför behöver 50 p § och 52 a § i lagen om Finansinspektionen ändras med avseende på dels Finansinspektionens roll som behörig myndighet enligt direktivet om nät- och informationssäkerhet när det gäller sektorerna 3 och 4 i bilaga II till direktivet, dels Finansinspektionens skyldighet att samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet. Finansinspektionens samarbete med Transport- och kommunikationsverket och verkets Cybersäkerhetscenter är även i fortsättningen viktigt för att främja cybersäkerheten och motståndskraften på finansmarknaden. Det är motiverat att fortsättningsvis betona vikten av myndighetssamarbete i lagstiftningen. Dessutom behöver CER-direktivet beaktas i bestämmelserna när det gäller sektorerna 3 och 4 i bilagan till direktivet. Även om skyldigheterna enligt CER-direktivet inte tillämpas på kritiska entiteter inom de sektorerna förutsätter direktivet att i synnerhet kritiska entiteter stöds för att förbättra deras motståndskraft.

3.5 Ändringar som DORA-ändringsdirektivet förutsätter i den nationella lagstiftningen

Som det konstateras ovan finns för närvarande bestämmelser om krav på finanssektorns IKT-riskhantering i flera av Europeiska parlamentets och rådets direktiv. Kraven varierar, och därmed varierar också de nationella bestämmelser som antagits för att genomföra dem. I DORA-ändringsdirektivet föreskrivs det om ändringar för att säkerställa att regleringen är konsekvent med EU:s DORA-förordning. Med anledning av bestämmelserna i direktivet behövs ändringar i 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 tilläggspensionsstiftelser och tilläggspensionskassor (947/2021) och försäkringsbolagslagen (521/2008). I praktiken handlar dessa ändringar i huvudsak om kraven på att förvalta nät- och informationssystem i enlighet med EU:s DORA-förordning som en del av den interna styrningen och riskhanteringsförfarandena. Dessutom har regleringen om planer för driftskontinuitet preciserats, i fråga om kreditinstitut i kreditinstitutsdirektivet och i fråga om värdepappersföretag som bedriver algoritmisk handel samt reglerade marknader i MiFID II-direktivet, så att dessa planer inbegriper IKT-kontinuitetspolicyer och planer samt åtgärds- och återställningsplaner avseende IKT i enlighet med EU:s DORA-förordning. Eftersom förordningen är direkt tillämplig rätt för dessa finansiella entiteter är sådana bestämmelser i huvudsak informativa, och därmed räcker det huvudsakligen med att ta in behövliga hänvisningar till EU:s DORA-förordning i de bestämmelserna för att genomföra DORA-ändringsdirektivet.

DORA-ändringsdirektivet förutsätter också vissa innehållsliga ändringar i den nationella lagstiftningen. Som det konstateras ovan har kreditinstitutsdirektivet ändrats så att en behörig myndighet ska ha rätt att kräva all information den behöver för att kunna utföra sina uppgifter

också av tredjepartsleverantörer av IKT-tjänster. Detta ska enligt förslaget genomföras genom en ändring av lagen om Finansinspektionen. Dessutom har tillämpningsområdet för översyns- och utvärderingsprocessen enligt kreditinstitutsdirektivet ändrats så att risker som påvisats vid testning av digital operativ motståndskraft enligt kapitel IV i EU:s DORA-förordning ska beaktas vid utvärderingen. Kreditinstitutslagen ska preciseras till den delen. Bestämmelserna om incidentrapportering i artikel 96.1–5 i betaltjänstdirektivet tillämpas i fortsättningen inte på betaltjänstleverantörer som omfattas av tillämpningsområdet för EU:s DORA-förordning. Till den delen behöver lagen om betalningsinstitut ändras.

Nedan beskrivs de bestämmelser i DORA-ändringsdirektivet som inte förutsätter några ändringar i nationella bestämmelser på lagnivå. I övrigt beskrivs genomförandet av respektive bestämmelse i DORA-ändringsdirektivet närmare i specialmotiveringen till lagförslagen.

Artikel 7.1 i DORA-ändringsdirektivet, som ersätter begreppet ”informationsteknik” med begreppet ”informations- och kommunikationsteknik” i betaltjänstdirektivets artikel 3 j om att tjänster som stöder tillhandahållandet av betaltjänster inte ska omfattas av direktivets tillämpningsområde, förutsätter inga ändringar i den nationella lagstiftningen. Till den delen har begränsningen av tillämpningsområdet genomförts genom specialmotiveringen till lagen om betalningsinstitut (RP 172/2009 rd, s. 30). Inte heller artikel 7.3 i DORA-ändringsdirektivet, som ersätter begreppet ”it-system” med begreppet ”IKT-system” i artikel 19.6 andra stycket i betaltjänstdirektivet, förutsätter några nationella genomförandeåtgärder. IKT-system nämns som ett exempel på viktiga operativa funktioner, som endast får utkontrakteras under vissa förutsättningar. Detta nämns inte som ett exempel i den nationella lagen.

Artikel 5.1 c och 7.6 i DORA-ändringsdirektivet gäller EBA:s tekniska standarder och förutsätter därmed inga ändringar i den nationella lagstiftningen. Direktivets artikel 5, med undantag för punkt 1 led c, och artikel 7.2 rör i sin tur frågor som nationellt regleras på förordningsnivå. I avsnitt 7 (Bestämmelser på lägre nivå än lag) beskrivs de ändringar som direktivet förutsätter i nationella bestämmelser på förordningsnivå.

Direktivet föranleder inga ändringsbehov i den nationella lagstiftningen till den del som vissa befogenheter att anta delegerade akter och genomförandeakter ändras genom DORA-ändringsdirektivet så att bestämmelserna om IKT-risk undantas från tillämpningsområdet för befogenheterna (direktivets artikel 1.2, 2.2, 3 i fråga om artikel 18.2 i AIFM-direktivet samt artikel 6.2 b och 6.4 c).

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

I lagen om Finansinspektionen föreslås de ändringar som föranleds av EU:s DORA-förordning samt ändringar som kompletterar det nationella genomförandet av NIS 2- och CER-direktiven. I lagen föreslås bestämmelser om att Finansinspektionen ska vara behörig myndighet enligt EU:s DORA-förordning samt behörig myndighet enligt NIS 2-direktivet och CER-direktivet när det gäller bankverksamhet och finansmarknadsinfrastruktur.

Enligt förslaget utvidgas de särskilda uppgiftsområden som kompletterar Finansinspektionens allmänna uppgift så att Finansinspektionen också har till uppgift att främja cybersäkra tillvägagångssätt hos finansmarknadsaktörer samt främja kritiska aktörers motståndskraft.

Finansinspektionens skyldigheter att samarbeta med andra myndigheter i syfte att främja cybersäkerheten på nationell nivå och inom ramen för de EU-omfattande

samarbetsarrangemang som inrättats med stöd av EU-rättsakter föreslås bli samlade i en ny paragraf.

Det föreslås att bestämmelserna om administrativa påföljder i lagen om Finansinspektionen kompletteras med anledning av EU:s DORA-förordning. Finansinspektionen ska enligt förslaget kunna påföra den som försummar eller bryter mot sina skyldigheter enligt EU:s DORA-förordning en påföljdsavgift. Den som försummar eller bryter mot skyldigheten att ha en förenklad IKT-riskhanteringsram enligt förordningen ska kunna påföras en ordningsavgift. De tredjepartsleverantörer av IKT-tjänster som avses i EU:s DORA-förordning läggs till i förteckningen över i lagen avsedda andra finansmarknadsaktörer, och då omfattar Finansinspektionens allmänna befogenheter också dessa aktörer.

Lagen om aktiebolaget Fonden för industriellt samarbete Ab (291/1979) och lagen om statens specialfinansieringsbolag (443/1998) ändras så att Fonden för industriellt samarbete Ab och Finnvera Abp lämnas utanför tillämpningsområdet för EU:s DORA-förordning.

Dessutom genomförs DORA-ändringsdirektivet genom propositionen. De ändringar som direktivet förutsätter görs i kreditinstitutslagen, lagen om investeringstjänster, lagen om betalningsinstitut, lagen om handel med finansiella instrument, lagen om placeringsfonder, lagen om förvaltare av alternativa investeringsfonder, lagen om tilläggspensionsstiftelser och tilläggspensionskassor och försäkringsbolagslagen.

4.2 De huvudsakliga konsekvenserna

Ekonomiska konsekvenser

EU:s DORA-förordning är direkt tillämplig rätt i Finland, och de finansiella entiteter som omfattas av förordningens tillämpningsområde är skyldiga att följa bestämmelserna i förordningen utan särskilda nationella genomförandeåtgärder. De operativa och ekonomiska konsekvenserna för finansiella entiteter är därmed huvudsakligen direkta följder av bestämmelserna i förordningen. De bestämmelser som föreslås i denna proposition kompletterar EU:s DORA-förordning särskilt när det gäller Finansinspektionens uppgifter, befogenheter och påförande av administrativa påföljder. För de aktörer som omfattas av tillämpningsområdet för EU:s DORA-förordning föreslås inga nya skyldigheter eller skyldigheter som går utöver det som föreskrivs i förordningen. I detta sammanhang beskrivs dock kort EU-regleringens konsekvenser för aktörerna utifrån de konsekvensbedömningar som EU-kommissionen utarbetade i samband med förslaget till DORA-lagstiftning.

De viktigaste ekonomiska konsekvenserna av EU:s DORA-förordning gäller företag i finanssektorn, dem som utövar tillsyn över verksamheten i sektorn samt tredjepartsleverantörer av IKT-tjänster för finanssektorn. Enligt bedömningen kan förordningen också få ekonomiska konsekvenser för de finansiella aktörernas kunder, för investerare och för konsumenter. Regleringens ekonomiska konsekvenser kan vara av engångsnatur eller kontinuerliga. I Finland omfattas hundratals olika stora aktörer, som även i övrigt har olika struktur och affärsverksamhet, av förordningen och påverkas därmed också av regeringens proposition.

Beaktandet av och beredskapen inför cyberrisker är generellt på en god nivå i finanssektorn i Finland. Finansiella aktörer är skyldiga att beakta cyberrisker som en del av hanteringen av operativa risker, och har redan utvecklat åtgärder för beredskapen inför cyberrisker i syfte att fullgöra dessa skyldigheter. En del av kraven i EU:s DORA-förordning är dock nya eller preciserar miniminivån, och i det fallet kan uppdateringar och andra ändringar som behövs i

informationssystemen orsaka engångskostnader för de företag som använder dem. Dessutom måste hanteringen av IKT-risker tilldelas tillräckliga resurser för att de relaterade kraven fortlöpande ska kunna följas. I synnerhet för försäkringsmedlare är kraven dessutom helt nya eftersom deras operativa riskhantering inte tidigare har reglerats. Det är svårt att exakt uppskatta kostnaderna eftersom de bland annat beror på nivån på aktörernas IKT-system jämfört med kraven i EU:s DORA-förordning. Kostnaderna kommer dock sannolikt att vara moderata i Finland eftersom man kan utgå från att de stora aktörernas IKT-system och riskhanteringsförfaranden i stor utsträckning redan uppfyller kraven, medan mindre strikta krav tillämpas på de mindre aktörerna i enlighet med proportionalitetsprincipen.

EU:s DORA-förordning syftar till att förenkla och harmonisera testningskraven på IKT-system och rapporteringen av IKT-incidenter i unionen. I sin bedömning konstaterade de europeiska tillsynsmyndigheterna att de löpande kostnaderna för hotbildsstyrd penetrationstestning utgör 0,1–0,3 procent av de berörda företagens hela IKT-budget. Harmoniserade testningsförfaranden gynnar särskilt gränsöverskridande banker – de 44 största av dem kan uppnå en nytta på hela 11–88 miljoner euro på årsnivå. När överlappande incidentrapporteringskrav slopas minskar i sin tur särskilt de stora bankernas administrativa börda, vilket kan innebära årliga besparingar på 40–100 miljoner euro på unionsnivå för dem.

Genomförandet av EU:s DORA-förordning uppskattas minska de direkta kostnaderna för cyberincidenter och potentiellt även generellt de negativa effekterna för den finansiella stabiliteten. I kommissionens konsekvensbedömning uppskattades de negativa konsekvenserna av cyberincidenter, under förutsättning att en av fem cyberincidenter inträffar inom finanssektorn, på unionsnivå 2018 till totalt 2–27 miljarder amerikanska dollar. Om man tillämpar dessa uppskattningar och antaganden av kommissionen kan man konstatera att summan av de negativa konsekvenserna av cyberincidenter 2018 i Finland var uppskattningsvis 2,9–39 miljoner amerikanska dollar. Om man lyckas minska konsekvenserna ens med tio procent innebär det i Finland en årlig besparing på 0,29–3,9 miljoner amerikanska dollar. Enligt kommissionen är en minskning med tio procent realistisk, men effekten kan bli större än så. Kommissionen betonar i sin bedömning att det är mycket svårt att bedöma konsekvenserna i det avseendet, eftersom incidenterna inte har rapporterats heltäckande och det ofta är oklart vilka direkta och indirekta kostnader som inkluderats i kostnaderna för incidenter.

Tillsynsmyndigheternas extra uppgifter till följd av skyldigheterna enligt EU:s DORA-förordning bedöms orsaka de berörda myndigheterna ringa kostnader för personalökningar. Mängden arbete kan öka till exempel på grund av ett ökande antal incidentrapporter. Enligt kommissionens bedömning kommer den ledande myndighetens heltidsanställda att öka med 1–5 personer och de deltagande myndigheternas med i genomsnitt 0,25 personer till följd av uppgifterna som tillsynen över tredjepartsleverantörer av IKT-tjänster medför.

Tredjepartsleverantörernas verksamhet kan enligt bedömningen påverkas av de ekonomiska konsekvenserna av EU:s DORA-förordning till följd av att tillsynsmyndigheterna ålägger dem att ändra sina system så att de överensstämmer med skyldigheterna enligt EU:s DORA-förordning. Tredjepartsleverantörerna av IKT-tjänster ska också anpassa sina organisationer för att möjliggöra tillsynen över sin verksamhet så att den passar in i ramverket av skyldigheter enligt EU:s DORA-förordning, vilket kommer att medföra kostnader. Enligt kommissionens bedömning kommer dessa kostnader dock att vara moderata, framför allt om det i framtiden byggs upp ett horisontellt branschspecifikt tillsynssystem för tredjepartsleverantörer av IKT-tjänster.

De finansiella aktörernas kunder, investerare och konsumenter kan påverkas av marginella ekonomiska konsekvenser. Enligt bedömningen är det möjligt att företag i finanssektorn i

slutändan finansierar en del av kostnaderna för genomförandet av EU:s DORA-förordning genom olika höjningar av kund- och serviceavgifterna.

Konsekvenser för myndigheternas verksamhet

EU:s DORA-förordning och den övriga lagstiftningen om digital operativ motståndskraft ställer krav på Finansinspektionens verksamhet. Olika informations- och kommunikationstekniska system är kritiska för de finansiella entiteternas dagliga verksamhet och därmed också en betydande källa till operativ risk. EU:s DORA-förordning syftar i sista hand till att säkerställa finansiell stabilitet och marknadsintegritet. För att regleringen ska kunna genomföras effektivt måste tillsynsmyndigheten också anvisa tillräckliga resurser för tillsynen och stödet för finansiella aktörer i frågor som gäller digital operativ motståndskraft. Genom förslagen preciseras Finansinspektionens skyldigheter i egenskap av tillsynsmyndighet för finansmarknaden och behörig myndighet enligt det gällande direktivet om nät- och informationssäkerhet. Även myndighetssamarbete på nationell och internationell nivå hör redan nu till Finansinspektionens uppgifter. Bestämmelserna om myndighetssamarbete och informationsutbyte i EU:s DORA-förordning ställer emellertid allt mer detaljerade krav också på Finansinspektionens verksamhet, till exempel i form av nya samarbetsstrukturer på EU-nivå. Bland annat ska en företrädare för Finansinspektionen delta i det tillsynsforum som ingår i tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster, och efter behov i verksamheten i samarbetsgruppen enligt NIS 2-direktivet. I princip ska Finansinspektionen sköta uppgifterna inom ramen för sina nuvarande resurser, genom att vid behov rikta om befintliga resurser till uppgifter som föranleds av EU:s DORA-förordning, och besluta närmare om tillsynen över att skyldigheterna enligt förordningen fullgörs och om prioriteringarna i tillsynen. I och med att bestämmelserna träder i kraft behövs dock uppföljning och bedömning av huruvida Finansinspektionens resurser är tillräckliga för att den ska kunna utföra sina uppgifter.

Syftet med förslagen om myndighetssamarbete enligt denna proposition är att betona det aktiva myndighetssamarbetets betydelse med tanke på en resultatrik skötsel av uppgifterna i anslutning till cybersäkerheten och att klargöra ordnandet av samarbetet mellan Finansinspektionen och andra myndigheter. I sista hand ska Finansinspektionen och de övriga myndigheter som deltar i samarbetet sinsemellan fastställa samarbetsformerna och den närmare praxisen för samarbetet, till den del det inte särskilt har föreskrivits närmare om samarbetet. För att främja sektorsövergripande samordning av cybersäkerheten är det särskilt viktigt att Finansinspektionen förmedlar mottagna störningsanmälningar utan obefogat dröjsmål till Cybersäkerhetscentret vid Transport- och kommunikationsverket.

EU:s DORA-förordning har också konsekvenser för verksamheten vid den nationella resolutionsmyndigheten, Verket för finansiell stabilitet. Verket för finansiell stabilitet deltar i myndighetssamarbetet för att främja cybersäkerhet och operativ motståndskraft och måste för att kunna utföra sina lagstadgade uppgifter ha en heltäckande lägesbild av det aktuella cybersäkerhetsläget i synnerhet för de kreditinstitut och värdepappersföretag som omfattas av verkets befogenheter. Behovet av ett effektivare informationsutbyte mellan de berörda myndigheterna, inbegripet resolutionsmyndigheterna, betonas också i ingressen till förordningen. Finansinspektionen och Verket för finansiell stabilitet ska ha lämpliga arrangemang för informationsutbyte så att verket vid rätt tidpunkt har tillgång till de uppgifter som behövs för att det ska kunna utföra sina uppgifter.

Lagstiftningen om digital operativ motståndskraft ska beaktas bland annat vid bedömning av avvecklings- och omorganiseringsmöjligheter enligt 3 kap. i lagen om resolution av

kreditinstitut och värdepappersföretag (1194/2014). I fortsättningen måste man i bedömningen bland annat beakta den digitala operativa motståndskraften för nät- och informationssystem som stöder institutets kritiska funktioner och kärnverksamhetsområden, med hänsyn till rapporter om allvarliga IKT-relaterade incidenter och resultat av testning av den digitala operativa motståndskraften i enlighet med EU:s DORA-förordning. Kreditinstituten och värdepappersföretagen bör säkerställa att relevanta avtal för IKT-tjänster är solida och kan hävdas i händelse av resolution av dessa finansiella entiteter, och Verket för finansiell stabilitet ska bedöma hur detta krav uppfylls vid sin bedömning av möjligheterna till avveckling och omorganisering av institutet eller koncernen. Avtalen om IKT-tjänster ska innehålla klausuler om att de inte får sägas upp, inte får upphävas tillfälligt och inte ändras på grund av omstrukturering eller resolution, så länge som de finansiella entiteterna fortsätter att uppfylla sina betalningsskyldigheter. Enligt artikel 30.2 i EU:s DORA-förordning ska de kontraktsmässiga arrangemangen för användning av IKT-tjänster innehålla bland annat skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med resolutionsmyndigheterna samt uppsägningsrätt och tillhörande minsta uppsägningstid för uppsägning av det kontraktsmässiga arrangemanget, i enlighet med de behöriga myndigheternas och resolutionsmyndigheternas förväntningar.

Andra konsekvenser för enskilda och för samhället

I och med genomförandet av EU:s DORA-förordning kan det generella förtroendet för finansmarknaden bedömas öka, vilket i det långa loppet gynnar alla marknadsparter. När kraven på digital operativ motståndskraft är enhetliga i hela unionen bedöms investerarnas förtroende för de finansiella aktörernas stabilitet förbli högt och deras vilja att investera i lösningar som är viktiga för att upprätthålla och utveckla cybersäkerheten förbli stark.

När de finansiella aktörernas digitala operativa motståndskraft upprätthålls och utvecklas säkerställer man också ett starkt skydd för konsumenter och investerare. När sektorns aktörer kan skydda sig mot cyberattacker och cyberincidenter kan de också säkerställa kontinuiteten i sina dagliga funktioner, en effektiv service för kunder och investerare samt skyddet av deras information och tillgångar.

5 Alternativa handlingsvägar

5.1 Den behöriga myndighetens befogenheter samt administrativa påföljder

Artikel 50 i EU:s DORA-förordning förutsätter på det sätt som beskrivs närmare ovan att de behöriga myndigheterna ska ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen. Medlemsstaterna ska fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen och säkerställa att de genomförs effektivt. De föreskrivna sanktionerna och åtgärderna ska vara effektiva, proportionella och avskräckande. Enligt artikel 51.1 i förordningen ska de behöriga myndigheterna dessutom utöva sina befogenheter att ålägga de administrativa sanktioner och avhjälpande åtgärder som avses i artikel 50 i enlighet med sina nationella rättsliga ramar. Enligt artikel 52 i förordningen får medlemsstaterna besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt.

Medlemsstaterna avgör på vilket sätt de säkerställer att kraven i artikel 50–52 i EU:s DORA-förordning uppfylls i den nationella lagstiftningen. I den mån det är möjligt kan förordningens krav uppfyllas genom den gällande lagstiftningen. Enligt utgångspunkten för denna proposition

eftersträvas ett så litet antal nya bestämmelser som möjligt. Finansinspektionen är i Finland den behöriga myndighet som avses i förordningen. Lagen om Finansinspektionen innehåller omfattande bestämmelser om Finansinspektionens tillsynsbefogenheter och de bedöms uppfylla förutsättningarna i förordningen. Därmed föreslås inga nya tillsynsbefogenheter för Finansinspektionen i denna proposition. Att ta in tredjepartsleverantörer av IKT-tjänster i förteckningen över andra finansmarknadsaktörer i lagen om Finansinspektionen är lagstiftningstekniskt det enklaste sättet att utsträcka Finansinspektionens behövliga tillsynsbefogenheter till att omfatta också dessa aktörer.

I bestämmelserna om Finansinspektionens ordningsavgift och påföljdsavgift anges vilka bestämmelser som ska ha försummats eller brutits mot för att påföljden ska kunna påföras. Dessa bestämmelser bör kompletteras så att en påföljd kan påföras den som försummar eller bryter mot de relevanta bestämmelserna i EU:s DORA-förordning. Utan uttryckliga bestämmelser kan Finansinspektionen inte påföra några andra administrativa påföljder än offentlig varning enligt 39 § i lagen om Finansinspektionen. Detta kan inte betraktas som tillräckligt eftersom EU:s DORA-förordning också förutsätter ekonomiska sanktioner som en möjlighet. I regeringens proposition föreslås det att Finansinspektionen ska kunna påföra en påföljdsavgift för försummelse av eller brott mot artiklarna 5–14, 17–19, 24–27 eller 28–30 i EU:s DORA-förordning. Om det felaktiga förfarandet kan anses vara obetydligt kan Finansinspektionen meddela en offentlig varning i stället för att påföra en påföljdsavgift, vilket bidrar till att trygga regleringens proportionalitet. Den som försummar eller bryter mot bestämmelserna om en förenklad IKT-riskhanteringsram enligt artikel 16 i förordningen ska i sin tur kunna påföras en lindrigare påföljd, det vill säga en ordningsavgift. Alternativa regleringssätt skulle till exempel vara att alla brott mot skyldigheterna enligt EU:s DORA-förordning endast skulle medföra sanktionen ordningsavgift, eller att också brott mot skyldigheten att ha en förenklad IKT-riskhanteringsram skulle medföra en påföljdsavgift som sanktion. Det sätt som föreslås i regeringens proposition bedöms dock bäst trygga dels regleringens effektivitet och avskräckande effekt, dels regleringens proportionalitet. Det föreslås inte några bestämmelser om att brott mot skyldigheterna enligt EU:s DORA-förordning ska vara straffrättsligt straffbara, eftersom förordningen inte förutsätter det och administrativa påföljder kan bedömas vara tillräckliga.

5.2 Rapportering om IKT-relaterade incidenter

Finansiella entiteter ska rapportera allvarliga IKT-relaterade incidenter till den behöriga myndigheten enligt artikel 19 i EU:s DORA-förordning. Enligt artikel 19.1 sjätte stycket får medlemsstaterna även besluta att vissa eller alla finansiella entiteter dessutom ska lämna alla de anmälningar och rapporter som avses i artikeln till de CSIRT-enheter för hantering av it-säkerhetsincidenter som utsetts eller inrättats i enlighet med NIS 2-direktivet. Cybersäkerhetscentret vid Transport- och kommunikationsverket är i Finland CSIRT-enhet i enlighet med NIS 2-direktivet. Finansiella entiteter kan alltså åläggas att rapportera incidenter förutom till Finansinspektionen också till Cybersäkerhetscentret, som då får vetskap om incidentanmälningar samtidigt som Finansinspektionen. För att undvika överlappande rapporteringsskyldigheter, och eftersom den behöriga myndigheten i vilket fall som helst i god tid ska lämna detaljerade uppgifter om allvarliga IKT-relaterade incidenter också till CSIRT-enheten, föreslås det inte i regeringens proposition att denna ytterligare rapporteringsskyldighet ska införas.

Enligt artikel 19.2 tredje stycket i EU:s DORA-förordning får medlemsstaterna fastställa att de finansiella entiteter som rapporterar på frivillig basis om betydande cyberhot också får vidarebefordra den anmälan till CSIRT-enheten. Regeringens proposition innehåller inga förslag om detta, och frågan behöver över huvud taget inte regleras på lagnivå.

5.3 Institut som är befriade med stöd av kreditinstitutsdirektivet

Enligt artikel 2.4 i EU:s DORA-förordning får medlemsstaterna från tillämpningsområdet för förordningen utesluta sådana enheter som avses i artikel 2.5.4–2.5.23 i kreditinstitutsdirektivet, om de är belägna inom deras respektive territorier. Om medlemsstaten beslutar att inte tillämpa det alternativ som avses i förordningens artikel 2.4 tillämpas den förenklade IKT-riskhanteringsramen enligt förordningens artikel 16 på sådana enheter. Med stöd av artikel 46 i förordningen ska den behöriga myndigheten enligt kreditinstitutsdirektivet, i Finland Finansinspektionen, dessutom säkerställa att dessa aktörer fullgör sina skyldigheter enligt förordningen i enlighet med de befogenheter som tilldelats genom respektive rättsakt. För Finlands del gäller denna option Fonden för industriellt samarbete Ab och Finnvera Abp. Fonden för industriellt samarbete Ab, det vill säga Finnfund, hör till utrikesministeriets förvaltningsområde och bestämmelser om fondens verksamhet finns i lagen om aktiebolaget Fonden för industriellt samarbete Ab. Finnvera Abp hör till arbets- och näringsministeriets förvaltningsområde och bestämmelser om dess verksamhet finns i lagen om statens specialfinansieringsbolag. Kreditinstitutslagen tillämpas inte på någondera av aktörerna och för närvarande övervakar inte Finansinspektionen deras verksamhet.

I regeringens proposition föreslås det att medlemsstaternas ovannämnda option utnyttjas. Fonden för industriellt samarbete Ab och Finnvera Abp lämnas alltså utanför tillämpningsområdet för EU:s DORA-förordning. Om medlemsstatsoptionen inte utnyttjas, ska det i detta sammanhang föreskrivas om Finansinspektionens uppgift att övervaka att Fonden för industriellt samarbete Ab och Finnvera Abp fullgör skyldigheterna enligt EU:s DORA-förordning samt om behövliga tillsynsbefogenheter och tillsynsavgifter som tas ut av aktörerna i anslutning till detta. Det kan inte anses ändamålsenligt att skapa separata tillsynsarrangemang i fråga om en enskild rättsakt, utan styrningen och tillsynen av aktörerna bör bedömas som en helhet i samband med att lagstiftningen om dem revideras. Lagrevideringsprojekt som gäller såväl Fonden för industriellt samarbete Ab som Finnvera Abp pågår för närvarande, och i samband med det kan man i sak bedöma tillämpningen av EU:s DORA-förordning på de aktörerna. Med hjälp av ägarstyrning kan man också se till att Fonden för industriellt samarbete Ab och Finnvera Abp i sin verksamhet följer IKT-riskhanteringsförfaranden som till art och omfattning motsvarar skyldigheterna enligt EU:s DORA-förordning trots att de inte omfattas av förordningens tillämpningsområde.

5.4 Behörigheter och uppgifter som gäller hotbildsstyrd penetrationstestning

Enligt artikel 26.9 i EU:s DORA-förordning får medlemsstaterna utse en enda offentlig myndighet inom finanssektorn som ska ansvara för frågor som rör hotbildsstyrd penetrationstestning inom den finansiella sektorn på nationell nivå och ska ge myndigheten alla befogenheter och uppgifter i detta syfte. Om det inte har utsetts någon myndighet, och utan att det påverkar befogenheten att välja ut vilka finansiella entiteter som är skyldiga att utföra hotbildsstyrd penetrationstestning, får en behörig myndighet med stöd av punkt 10 delegera vissa eller alla av de uppgifter som avses i artikel 26 och 27 i EU:s DORA-förordning till en annan nationell myndighet inom den finansiella sektorn.

I det avseendet förutsätter EU:s DORA-förordning alltså inga nationella bestämmelser. I praktiken kan den andra nationella myndighet inom den finansiella sektorn som avses i förordningen i Finlands fall vara Finlands Bank, som för närvarande ansvarar för TIBER-FI-modellen. De alternativa lagstiftningslösningarna är att antingen föreskriva att Finansinspektionen eller Finlands Bank ska ha till uppgift att ansvara för frågor som rör hotbildsstyrd penetrationstestning på nationell nivå eller låta bli att utse en myndighet enligt artikel 26.9 i förordningen. Som det beskrivs ovan är det i princip motiverat att

Finansinspektionen ska ansvara för tillsynsuppgifterna i anslutning till hotbildsstyrd penetrationstestning. Finlands Bank föreslås även i fortsättningen ansvara för förvaltningen av den modell som används vid testningen. Uppgifterna enligt artiklarna 26 och 27 i förordningen inbegriper också utövning av offentlig makt, och därför måste myndighetsuppgifterna och de relaterade befogenheterna anges tydligt i lagstiftningen. Därmed är det motiverat att utse Finansinspektionen till den myndighet som avses i artikel 26.9 i EU:s DORA-förordning.

6 Remissvar

Inställningen till utkastet till regeringens proposition var positiv i de yttranden som gavs. Samtidigt framfördes flera iakttagelser om detaljer i utkastet och förslag till kompletteringar av propositionen. Nedan beskrivs hur dessa iakttagelser och förslag har beaktats i den fortsatta beredningen av regeringens proposition.

Justitieministeriet och justitiekanslersämbetet framhävde att tillsynsmyndigheternas befogenheter bör definieras tydligt i bestämmelser som kompletterar EU:s DORA-förordning. Justitieministeriet fäste uppmärksamhet vid den vaga formuleringen av fastställandet av de parter som deltar i samarbetet i den föreslagna 3 f § i lagen om Finansinspektionen och vid bedömningen av tillräckliga rättigheter att få information för genomförandet av myndighetssamarbetet. Dessutom konstaterade justitieministeriet och justitiekanslersämbetet att det förblir oklart i den föreslagna 71 § 1 mom. 20 punkten vilken information som ska kunna lämnas ut till Transport- och kommunikationsverket trots sekretessbestämmelserna. Justitieministeriet tog upp att det är oklart i vilken mån Finansinspektionens tillsynsbefogenheter omfattar tredjepartsleverantörer av IKT-tjänster, och uppmanade beredarna att överväga ett tydligare regleringssätt i den fortsatta beredningen. Dessutom ansåg justitieministeriet och justitiekanslersämbetet att förslagen om administrativa påföljder bör motiveras ännu närmare. I utkastet till proposition föreslås delvis bestämmelser om en påföljdsavgift för försummelse av eller brott mot bestämmelser som är förpliktande för myndigheterna. Även Finanssiala ry fäste uppmärksamhet vid kraven i fråga om administrativa påföljder. Justitiekanslersämbetet ansåg att valet att lämna Fonden för industriellt samarbete Ab och Finnvera Abp utanför tillämpningsområdet för EU:s DORA-förordning bör motiveras ännu närmare.

Specialmotiveringen till lagförslagen kompletterades i behövliga delar för att beakta de synpunkter och oklarheter som beskrivs ovan. Formuleringen av den föreslagna nya 40 § 2 mom. 13 punkten i lagen om Finansinspektionen preciserades för att det ska vara klart vilka bestämmelser som ska ha brutits mot för att en påföljdsavgift ska kunna påföras. I den föreslagna nya 71 § 1 mom. 20 punkten preciserades dessutom den information som bestämmelsen gäller. Motiveringen till lagstiftningsordningen har också kompletterats i propositionen i fråga om administrativa påföljder och bestämmelserna om utlämnande av information.

Finansinspektionen föreslog att bemyndigandet att meddela föreskrifter i 18 § i lagen om Finansinspektionen kompletteras så att det omfattar den fortlöpande skyldigheten att rapportera IKT-incidenter. Propositionen ändrades inte till den delen i den fortsatta beredningen. Med stöd av den gällande lagstiftningen har Finansinspektionen meddelat föreskrifter bland annat om lämnande av information om störningar till Finansinspektionen. I motiveringen till regeringens proposition konstateras att bestämmelserna inte bör inbegripa rapporteringsskyldigheter som överlappar med EU:s DORA-förordning, men i övrigt är avsikten inte att i samband med propositionen ändra rapporteringsskyldigheter som grundar sig på nationell lagstiftning. Finansinspektionens syn är att krav på digital operativ motståndskraft motsvarande EU:s DORA-förordning bör föreskrivas även för arbetspensionsförsäkringsbolag och vissa andra

aktörer. Propositionen ändrades inte till den delen i den fortsatta beredningen. Arbetspensionsförsäkringsbolag omfattas inte av tillämpningsområdet för EU:s DORA-förordning, och i denna regeringsproposition tas inte ställning till frågor som gäller deras digitala operativa motståndskraft. När det gäller den föreslagna 44 § i lagen om Finansinspektionen ansåg Finansinspektionen att det vore bra att försöka placera bestämmelserna i anslutning till de relevanta paragraferna och att det borde framgå av dem att de bestämmelser i EU:s DORA-förordning som det hänvisas till ska tillämpas i stället för det som föreskrivs i lagen. I propositionens första lagförslag gjordes de ändringar som behövs i det avseendet.

Verket för finansiell stabilitet föreslog vissa nya bestämmelser om utlämnande av information med anknytning till förvaltningen av ett kontosystem inom försörjningsberedskapen. Propositionen ändrades inte till den delen i den fortsatta beredningen, eftersom Verket för finansiell stabilitet med stöd av den gällande lagstiftningen har rätt att av kreditinstitut få uppgifter som är nödvändiga för upprätthållandet av ett kontosystem inom försörjningsberedskapen. Verket har dessutom rätt att utan dröjsmål från bland annat Finansinspektionen få all information som är nödvändig för skötseln av verkets uppgifter.

När det gäller de befogenheter som rör hotbildsstyrd penetrationstestning konstaterade Finlands Bank att man i beredningen bör bedöma om det för Finlands Bank i praktiken uppstår en ny uppgift med grund i bestämmelserna, och om Europeiska centralbanken bör konsulteras i frågan i enlighet med rådets beslut 98/415/EG. Det första lagförslaget i propositionen ändrades för att förtydliga myndigheternas ansvarsområden så att de uppgifter enligt artikel 26 och 27 i EU:s DORA-förordning som rör hotbildsstyrd penetrationstestning hör till Finansinspektionens ansvarsområde.

Kommunikationsministeriet tog upp ett eventuellt behov av att föreskriva om samarbete mellan Finansinspektionen och andra myndigheter som övervakar att NIS 2-direktivet följs och om det relaterade informationsutbytet på samma sätt som mellan Finansinspektionen och Transport- och kommunikationsverket. Inrikesministeriet föreslog att man föreskriver om en skyldighet för Finansinspektionen att rapportera allvarliga IKT-incidenter till polisen, om incidenten misstänks bero på ett brott för vilket det strängaste föreskrivna straffet är fängelse i minst tre år. Till dessa delar ändrades inte regeringens proposition i den fortsatta beredningen. Finansinspektionen har inte ansett att det behövs mer omfattande bestämmelser om utlämnande av information. I princip är det enligt förslaget den finansiella entiteten som ansvarar för att vid behov till polisen rapportera cyberattacker som den utsatts för. Dessutom föreskrivs det i 3 c § i lagen om Finansinspektionen att Finansinspektionen är skyldig att underrätta behöriga myndigheter om eventuella brott. Transport- och kommunikationsverket föreslog att man överväger om det i regeringens proposition bör tas in en undantagsbestämmelse i förhållande till 136 § 4 mom. i lagen om tjänster inom elektronisk kommunikation för att finansiella entiteter inom ramen för arrangemangen för informationsutbyte enligt artikel 45.1 i EU:s DORA-förordning sinsemellan ska kunna utbyta också information som inbegriper förmedlingsuppgifter och uppgifter om innehållet i meddelanden. I den fortsatta beredningen bedömde man att den bestämmelsen kan tas in i den nya lag som föreslås för att genomföra NIS 2-direktivet. På grund av tidsplanerna för regeringens propositioner bereds den ändringen separat.

Verket för finansiell stabilitet ansåg att konsekvenserna för resolutionsmyndigheter bör beskrivas mer heltäckande i motiveringen till propositionen. Finanssiala ry ansåg att de kostnader som EU:s DORA-förordning orsakar för företag inom finanssektorn kan bli avsevärt högre än uppskattat. Dessutom ansåg Finanssiala ry att det är viktigt att realistiskt bedöma Finansinspektionens resursbehov och anvisa tillräckliga resurser för att den ska kunna utföra

sina uppgifter. Konsekvensbedömningarna i propositionen preciserades i den fortsatta beredningen för att beakta dessa synpunkter.

I det femte lagförslaget i propositionen beaktades Nasdaq Helsinki Oy:s förslag att ändringarna i 3 kap. 1 § 1 mom. i lagen om handel med finansiella instrument bör avgränsas så att de inte tillämpas på börsers holdingföretag. Dessutom preciserades motiveringen till lagförslaget. I det åttonde lagförslaget i propositionen preciserades det i enlighet med Eläkesäätiöyhdistys ESY ry:s förslag att det föreslagna 3 kap. 12 § 4 mom. i lagen om tilläggspensionsstiftelser och tilläggspensionskassor inte ska tillämpas på tilläggspensionsanstalter med färre än 16 försäkrade.

7 Specialmotivering

7.1 Lagen om Finansinspektionen

3 §. *Uppgifter*. I den gällande paragrafen föreskrivs det om Finansinspektionens uppgifter. I 1 mom. föreskrivs det om Finansinspektionen allmänna uppgift att utöva tillsyn över finansmarknadsaktörernas verksamhet enligt vad som föreskrivs i denna lag och i någon annan lag samt att dessutom främja goda förfaranden på finansmarknaden och allmänhetens kunskaper om finansmarknaden. Den allmänna uppgiften kompletteras av bestämmelserna i 2 och 3 mom. om Finansinspektionens särskilda uppgiftsområden. Till Finansinspektionens uppgifter hör bland annat att delta i det nationella samarbetet mellan myndigheter samt att delta inte bara i det samarbete inom Europeiska unionen som sker inom ramen för det europeiska systemet för finansiell tillsyn utan också i annat internationellt myndighetssamarbete.

På grund av den ökande samhälleliga betydelse som cybersäkerhet och motståndskraft på finansmarknaden har och på grund av den EU-lagstiftning som gäller dem är det skäl att precisera Finansinspektionens uppgifter med särskilda uppgifter att främja cybersäkra tillvägagångssätt hos finansmarknadsaktörer och kritiska aktörers motståndskraft. Finansmarknaden är en samhälleligt viktig institution vars föränderliga samhälleliga betydelse framgår av den ökande digitaliseringen och de informations- och kommunikationstekniska (IKT) lösningarnas kritiska betydelse för tillhandahållandet av finansiella tjänster, de ökade riskerna till följd av allvarlig it-brottslighet samt förändringen i Finlands säkerhetsmiljö. Av dessa orsaker är en hög nivå på cybersäkerheten hos alla finansmarknadsaktörer och bättre motståndskraft hos kritiska aktörer allt viktigare mål samhälleligt sett. Det är fråga om uppgifter i fråga om vilka det närmare innehållet och Finansinspektionens befogenheter i anslutning till dem bestäms enligt vad som föreskrivs om dem någon annanstans i lagstiftningen.

Enligt den föreslagna *nya 7 punkten* ska Finansinspektionen ha till uppgift att främja cybersäkra tillvägagångssätt hos finansmarknadsaktörerna. Enligt det föreslagna 50 p § 1 mom. ska Finansinspektionen vara den behöriga myndighet som avses i artikel 46 i EU:s DORA-förordning. Finansinspektionens uppgift som den myndighet som utövar tillsyn över EU:s DORA-förordning och deltar i samarbetsarrangemang enligt den utgör det viktigaste ledet i främjandet av cybersäkra tillvägagångssätt. Dessutom är Finansinspektionen den behöriga myndighet som avses i artikel 8.1 i NIS 2-direktivet när det gäller bankverksamhet och finansmarknadsinfrastruktur. Utöver sin tillsynsuppgift främjar Finansinspektionen cybersäkerheten bland annat genom att upprätthålla och dela en lägesbild över informationssäkerhetsincidenter och cyberattacker samt genom att delta i försörjningsberedskapsorganisationens verksamhet. Den sektorsöverskridande ömsesidiga spridningen av bland annat bästa praxis, cybersäkerhetskompetens och den mest aktuella informationen om nya former av cyberhot effektiviserar resursanvändningen och gagnar därmed också finansmarknadsaktörerna.

Enligt den föreslagna *nya 7 a-punkten* ska Finansinspektionen ha till uppgift att främja kritiska finansmarknadsaktörers motståndskraft. Finansinspektionen är den behöriga myndighet som avses i artikel 9.1 i CER-direktivet när det gäller bankverksamhet och finansmarknadsinfrastruktur. Artikel 10 i CER-direktivet förutsätter stöd till kritiska entiteter för att stärka deras motståndskraft och främja utbytet av information mellan dem. Enligt artiklarna 9.5 och 10.3 i direktivet ska den behöriga myndigheten när så är lämpligt samråda och samarbeta med kritiska entiteter och relevanta berörda parter.

Med tanke på de föreslagna nya uppgifterna är det viktigt med myndighetssamarbete för främjande av cybersäkerheten, som det föreskrivs närmare om i den föreslagna nya 3 f §, samt med informationsutbyte mellan de berörda myndigheterna.

3 f §. *Myndighetssamarbete för att främja cybersäkerhet och motståndskraft.* Det föreslås att det till lagen fogas *en ny 3 f §* med bestämmelser om Finansinspektionens skyldigheter att samarbeta med andra myndigheter för att främja cybersäkerheten på nationell nivå och inom ramen för de EU-omfattande samarbetsarrangemang som inrättats med stöd av EU-rättsakter. Myndighetssamarbete på nationell och internationell nivå hör redan nu till Finansinspektionens uppgifter. Syftet med paragrafen är att betona det aktiva myndighetssamarbetets betydelse med tanke på en resultatrik skötsel av uppgifterna i anslutning till cybersäkerheten och att klargöra ordnandet av samarbetet mellan Finansinspektionen och andra myndigheter. Kärnan i myndighetssamarbetet är samarbetet enligt EU:s DORA-förordning, inklusive samarbetet med de strukturer och myndigheter som inrättats genom NIS 2-direktivet, och på nationell nivå i synnerhet verksamheten med Cybersäkerhetscentret, som finns i anslutning till Transport- och kommunikationsverket, och dess CSIRT-funktion. Samarbetet omfattar i väsentlig grad också sådant informationsutbyte mellan myndigheterna, där den information som utbyts kan innehålla till exempel information om störningar i anslutning till informationssäkerheten och bästa praxis för att förebygga störningar och bemöta dem. Den allmänna samarbetsförpliktelsen medför inte i sig någon rätt att avvika från bestämmelserna om sekretessbelagd information. Utlämnande av sekretessbelagd information som en del av myndighetssamarbetet ska bedömas från fall till fall med stöd av de bestämmelser som tillämpas på ärendet.

I *1 mom*. föreslås allmänna bestämmelser om Finansinspektionens skyldighet att samarbeta med finansministeriet, social- och hälsovårdsministeriet, Finlands Bank, Verket för finansiell stabilitet, Transport- och kommunikationsverket och andra behöriga myndigheter för att hantera störningar relaterade till informations- och kommunikationsteknik och för att minska konsekvenserna av sådana störningar. Andra behövliga samarbetsparter kan vara bland annat de behöriga myndigheterna enligt NIS 2-direktivet inom andra i direktivet avsedda sektorer. Den föreslagna bestämmelsen kompletterar Finansinspektionens allmänna skyldighet enligt 3 § 3 mom. 6 punkten i lagen om Finansinspektionen att delta i det nationella samarbetet mellan myndigheter. Finansinspektionen och de övriga myndigheter som deltar i samarbetet ska sinsemellan fastställa samarbetsformerna och den närmare praxisen för samarbetet, till den del det inte särskilt har föreskrivits närmare om samarbetet.

I *2 mom*. föreslås bestämmelser om Finansinspektionens deltagande i samarbetet enligt artiklarna 32 och 47–49 i EU:s DORA-förordning. I artikel 32 i EU:s DORA-förordning ingår bestämmelser om tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster. Finansinspektionen ska delta i verksamheten i det tillsynsforum som ingår i tillsynsramen och utses till behörig myndighet i enlighet med artikel 32.5. I artikel 47 i EU:s DORA-förordning föreskrivs det om samarbetet på nationell nivå och EU-nivå med de strukturer och myndigheter som inrättats genom NIS 2-direktivet. Finansinspektionen får delta i verksamheten i den samarbetsgrupp som avses i NIS 2-direktivet i frågor som gäller dess tillsynsåtgärder i samband med finansiella institut. Finansinspektionen får också vid behov samråda och utbyta information

med de myndigheter som utsetts i enlighet med NIS 2-direktivet, nationellt alltså Transport- och kommunikationsverket och Cybersäkerhetscentret i anslutning till det, samt begära behövlig teknisk rådgivning och ingå samarbetsarrangemang. I artiklarna 48–49 i EU:s DORA-förordning föreskrivs det dessutom om andra former av internationellt myndighetssamarbete. De behöriga myndigheterna, de europeiska tillsynsmyndigheterna och ECB ska ha ett nära samarbete och utbyta information för att fullgöra sina uppgifter enligt EU:s DORA-förordning och de ska samordna sin tillsyn. Myndigheterna kan bland annat vid behov inrätta mekanismer för att möjliggöra utbyte av effektiv praxis mellan olika finansiella sektorer för att öka situationsmedvetenheten och identifiera gemensamma cybersårbarheter och cyberrisker inom olika sektorer. I det föreslagna momentet föreskrivs det dessutom att Finansinspektionen också i övrigt samarbetar med Europeiska centralbanken, Europeiska systemrisknämnden, Europeiska unionens cybersäkerhetsbyrå (ENISA), de europeiska tillsynsmyndigheterna, andra EU-myndigheter och utländska EES-tillsynsmyndigheter för att hantera störningar relaterade till informations-och kommunikationsteknik och för att minska konsekvenserna av sådana störningar. Finansinspektionen deltar dessutom i verksamheten inom det europeiska ramverket för samordning av åtgärder mot systemiska cyberincidenter. Ramverket baserar sig på Europeiska systemrisknämndens rekommendation ESRB/2021/17 av den 2 december 2021. Finansinspektionen har med stöd av gällande lagstiftning anmälts som nationell kontaktpunkt för ramverket i juni 2023.

Det föreslagna *3 mom*. ersätter 52 a §, som föreslås bli upphävd. I momentet föreskrivs det om Finansinspektionens skyldighet att samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt NIS 2-direktivet, genom vilket direktivet om nät- och informationssäkerhet upphävdes. Den föreslagna bestämmelsen kompletterar de ovannämnda bestämmelserna om myndighetssamarbete i EU:s DORA-förordning och betonar den särskilda betydelse som samarbetet mellan Finansinspektionen och Transport- och kommunikationsverket har. Transport- och kommunikationsverkets Cybersäkerhetscenter är i Finland en sådan gemensam kontaktpunkt och CSIRT-enhet som avses i NIS 2-direktivet. För att främja den sektorsövergripande samordningen av cybersäkerheten är det särskilt viktigt att Finansinspektionen utan obefogat dröjsmål förmedlar de inkomna störningsanmälningarna till Cybersäkerhetscentret så att det utifrån dem är möjligt att skapa en bättre helhetsbild av det rådande cybersäkerhetsläget. Bestämmelser om skyldigheten att lämna uppgifter om allvarliga IKT-relaterade incidenter finns i artikel 19.6 i EU:s DORA-förordning. Bestämmelser om Cybersäkerhetscentrets uppgifter finns i 3 § i lagen om Transport- och kommunikationsverket. Transport- och kommunikationsverket är också tillsynsmyndighet enligt NIS 2-direktivet inom sitt verksamhetsområde. Även behöriga myndigheter enligt NIS 2-direktivet inom andra i direktivet avsedda sektorer kan vara behövliga samarbetsparter för Finansinspektionen.

I det föreslagna *4 mom*. föreskrivs det om Finansinspektionens skyldighet att samarbeta med finansministeriet, inrikesministeriet, Försörjningsberedskapscentralen och andra behöriga myndigheter för skötseln av uppgifter enligt CER-direktivet, för att stärka kritiska aktörers motståndskraft och för att främja frivilligt informationsutbyte mellan dem.

Genom momentet kompletteras bestämmelserna i den nationella allmänna lag som utfärdas för genomförande av CER-direktivet när det gäller sektorerna 3 (bankverksamhet) och 4 (finansmarknadsinfrastruktur) i bilagan till direktivet. Enligt artikel 9.5 i CER-direktivet ska varje medlemsstat säkerställa att dess behöriga myndighet när så är lämpligt och i enlighet med unionsrätten och nationell rätt samråder och samarbetar med andra relevanta nationella myndigheter, inbegripet de som ansvarar för civilskydd, brottsbekämpning och skydd av personuppgifter, samt med kritiska entiteter och relevanta berörda parter. Enligt artikel 10.1 i CER-direktivet ska medlemsstaterna stödja kritiska entiteter för att stärka deras motståndskraft. Stödet får innefatta utveckling av vägledningsmaterial och metoder, stöd till anordnande av

övningar för att testa deras motståndskraft och tillhandahållande av rådgivning och utbildning för kritiska entiteters personal. Enligt artikel 10.3 ska dessutom frivillig informationsdelning mellan kritiska entiteter underlättas. Myndighetssamarbete är viktigt också för att undvika administrativa överlappningar, säkerställa att anvisningarna är heltäckande och stärka övningsverksamheten. Myndighetssamarbetet kan också omfatta beredskapsplanering, övningar eller annat myndighetssamarbete till exempel med försvarsmakten, polisen och räddningsväsendet. Även till dessa delar ska Finansinspektionen och de övriga myndigheter som deltar i samarbetet fastställa samarbetsformerna och den närmare praxisen för samarbetet.

5 §. *Andra finansmarknadsaktörer*. Genom den föreslagna ändringen läggs sådana tredjepartsleverantörer av IKT-tjänster som avses i EU:s DORA-förordning och som omfattas av dess tillämpningsområde till i förteckningen över andra finansmarknadsaktörer. Enligt artikel 3.19 i EU:s DORA-förordning avses med tredjepartsleverantörer av IKT-tjänster företag som tillhandahåller i förordningen avsedda IKT-tjänster.

Ändringen av bestämmelsen innebär att Finansinspektionens rätt att få uppgifter och granskningsrätt enligt 18–22 och 24 § och allmänna befogenheter enligt 33–34 § utsträcks till att omfatta tredjepartsleverantörer av IKT-tjänster. Till de allmänna befogenheterna hör verkställighetsförbud enligt 33 §, vite enligt 33 a § samt rätt att anlita utomstående sakkunniga enligt 34 §. Lagstiftningen innehåller redan nu vissa bestämmelser om detta. Finansinspektionens rätt enligt 18 § i den gällande lagen att få uppgifter av tillsynsobjekt och andra finansmarknadsaktörer samt granskningsrätten enligt 24 § gäller företag som på uppdrag av tillsynsobjekt eller andra finansmarknadsaktörer sköter uppgifter i anslutning till dessas datasystem.

Den föreslagna ändringen behövs eftersom det i skyldigheterna enligt EU:s DORA-förordning ingår att finansiella entiteter på behörigt sätt ska hantera IKT-tredjepartsrisker. Tillsynen över att förordningen efterlevs utsträcker sig således indirekt också till verksamhet som bedrivs av tredjepartsleverantörer av IKT-tjänster. I artikel 30 i förordningen föreskrivs det dessutom om de omständigheter som finansiella entiteter och tredjepartsleverantörer av IKT-tjänster ska beakta när de ingår avtal om dessa tjänster. EU:s DORA-förordning förutsätter att Finansinspektionen har alla befogenheter som krävs för att den ska kunna fullgöra sina skyldigheter enligt förordningen. Det att tredjepartsleverantörer av IKT-tjänster läggs till i förteckningen över andra finansmarknadsaktörer är lagstiftningstekniskt det enklaste sättet att utsträcka Finansinspektionens behövliga tillsynsbefogenheter till att omfatta också dessa aktörer. Samtidigt bör det beaktas att befogenheterna enligt lagstiftningen kan utövas endast när det behövs för skötseln av Finansinspektionens uppgifter. När det gäller tredjepartsleverantörer av IKT-tjänster kan särskilt rätten att få uppgifter och granskningsrätten bedömas vara centrala med tanke på den praktiska tillsynsverksamheten. Med stöd av vad som anförts ovan föreslås det inte att tredjepartsleverantörer av IKT-tjänster ska omfattas av avgiftsskyldigheten enligt lagen om Finansinspektionens tillsynsavgifter (1209/2023). EU:s DORA-förordning innehåller en separat tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster. I denna ram ingår också en tillsynsavgift som tas ut av den europeiska tillsynsmyndigheten.

Genom den föreslagna ändringen genomförs också den ändring av artikel 65.3 a vi i kreditinstitutsdirektivet som ingår i artikel 4.1 i DORA-ändringsdirektivet och enligt vilken den behöriga myndigheten ska ha rätt att ålägga också tredjepartsleverantörer av IKT-tjänster att lämna all information som behövs för att myndigheten ska kunna utföra sina uppgifter. I och med ändringen enligt DORA-ändringsdirektivet tillämpas också artikel 65.3 b och c i kreditinstitutsdirektivet på tredjepartsleverantörer av IKT-tjänster. Enligt de nämnda leden i artikeln ska den behöriga myndigheten ha befogenhet att genomföra alla nödvändiga utredningar av personer som avses i led a och som är etablerade eller belägna i den berörda

medlemsstaten, om detta är nödvändigt för att de behöriga myndigheterna ska kunna utföra sina uppgifter, samt befogenhet att, på de övriga villkor som anges i unionsrätten, genomföra alla nödvändiga kontroller i företagslokaler som tillhör de juridiska personer som avses i led a.

Enligt 7 kap. 4 § i lagen om myndigheten för finansiell stabilitet (1195/2014) ska en på finansmarknaden verksam juridisk person och fysiska personer i dess anställning, trots sekretessbestämmelserna, utan obefogat dröjsmål på begäran ge verket för finansiell stabilitet information och utredningar som är nödvändiga för att verket ska kunna sköta sina uppgifter enligt denna lag eller lagen om resolution av kreditinstitut och värdepappersföretag. Enligt 1 kap. 3 § 13 punkten i lagen om myndigheten för finansiell stabilitet avses med en juridisk person som agerar på finansmarknaden ett tillsynsobjekt enligt 4 § i lagen om Finansinspektionen eller en annan sådan finansmarknadsaktör som avses i 5 § i den lagen. Den föreslagna ändringen förtydligar således också kravet i artikel 30.2 g i EU:s DORA-förordning, enligt vilket ett avtal mellan en finansiell entitet och en tredjepartsleverantör av IKT-tjänster ska innehålla en skyldighet för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella entiteten.

38 §. *Ordningsavgift.* Till *1 mom*. fogas *en ny 12 punkt* enligt vilken Finansinspektionen kan ålägga den att betala ordningsavgift som uppsåtligen eller av oaktsamhet försummar eller bryter mot skyldigheten att hantera IKT-risker enligt artikel 16 i EU:s DORA-förordning. Den förenklade riskhanteringsramen enligt artikeln ska iakttas av de aktörer på finansmarknaden som har den minsta storleken och minsta systemiska betydelsen. En sådan här överträdelse ska anses vara ringa, och därför är det i regel inte behövligt att till följd av den påföra en påföljdsavgift som är ämnad för mer klandervärda förseelser och försummelser. Sanktioner behövs dock också i dessa fall framför allt för att trygga finansmarknadens allmänna tillförlitlighet. Dessutom kan det i särskilt klandervärda fall med stöd av 4 mom. påföras en påföljdsavgift i stället för en ordningsavgift. En sådan situation kan uppstå till exempel om en aktör helt och hållet underlåter att iaktta skyldigheten att hantera IKT-risker. Bestämmelsen baserar sig på artikel 50.3 i EU:s DORA-förordning, som förutsätter att medlemsstaterna inför lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen. Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande. I 1 mom. *11 punkten* görs samtidigt en teknisk ändring med anledning av den nya 12 punkten.

I *2 mom*. anges det vilka omständigheter som ska beaktas vid bedömningen av ordningsavgiftens belopp. Artikel 51.2 i EU:s DORA-förordning innehåller direkt tillämpliga bestämmelser om de omständigheter som den behöriga myndigheten ska ta hänsyn till när den fastställer administrativa sanktioner på grund av en överträdelse av förordningen. Det föreslås därför att det till paragrafen fogas *ett nytt 7 mom*. där det föreskrivs att artikel 51.2 i EU:s DORA-förordning ska iakttas i stället för 2 mom. i fråga om de omständigheter som ska beaktas vid bedömningen av ordningsavgiftens belopp, om det är fråga om en överträdelse av EU:s DORA-förordning. I 2 mom. föreskrivs det också om ordningsavgiftens maximibelopp. I EU:s DORA-förordning finns det inga bestämmelser om maximibeloppen för administrativa påföljder, och därför kan maximibeloppen enligt 2 mom. tillämpas också i dessa fall.

Dessutom föreskrivs det i 42 § 2 mom. att ordningsavgift inte kan påföras en person som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som behandlas i domstol och inte heller den som har dömts för samma gärning genom en lagakraftvunnen dom.

40 §. *Påföljdsavgift.* I *den nya 2 mom. 13 punkten* föreslås bestämmelser om Finansinspektionens behörighet att påföra en påföljdsavgift, om någon uppsåtligen eller av oaktsamhet försummar eller bryter mot de bestämmelser i artiklarna 5–14, 17–19, 24–27 eller

28–30 i EU:s DORA-förordning som är förpliktande för i artikel 2.2 i den förordningen avsedda finansiella entiteter. Bestämmelsen baserar sig på artikel 50.3 i EU:s DORA-förordning, som förutsätter att medlemsstaterna inför lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen. Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande. I *11* och *12 punkten* görs dessutom behövliga tekniska ändringar.

Den föreslagna bestämmelsen motsvarar de bestämmelser som gäller andra sektorer inom finansmarknaden. Av bestämmelsen framgår att Finansinspektionen i princip är skyldig att påföra en påföljdsavgift under de förutsättningar som anges i lagen. Med tanke på den samhälleliga betydelse som bestämmelserna om digital motståndskraft inom finanssektorn har och med tanke på att tillsynen över finansmarknaden ska vara trovärdig är det viktigt att Finansinspektionen har tillgång till effektiva sanktioner i fall där skyldigheterna enligt EU:s DORA-förordning överträds eller försummas. Därför är det motiverat att en påföljdsavgift påförs i dessa fall. Samtidigt är det ytterst viktigt att det tas hänsyn till de att administrativa påföljderna ska vara proportionella. Påföljdsavgift är en allvarlig administrativ påföljd, där de överträdelser och försummelser på vilka påföljden tillämpas i princip betraktas som synnerligen klandervärda (RP 32/2012 rd, s. 85). I sin eventuella påföljdsprövning beaktar Finansinspektionen de rättsprinciper inom förvaltningen som avses i 6 § i förvaltningslagen samt bestämmelserna om påförande av och avstående från en administrativ påföljd i lagen om Finansinspektionen och EU:s DORA-förordning. Vid prövningen av om en administrativ påföljd ska påföras ska hänsyn tas till alla relevanta omständigheter, såsom graden av uppsåt och överträdelsens väsentlighet och svårighetsgrad. Vid bedömningen av fullgörandet av skyldigheterna enligt EU:s DORA-förordning ska man i enlighet med proportionalitetsprincipen i artikel 4 i förordningen också ta hänsyn till bland annat den finansiella entitetens storlek och ekonomiska ställning. Bedömningen av den administrativa påföljdens proportionalitet gäller inte bara dimensioneringen av påföljdsavgiften, utan också valet av påföljdstyp. I stället för en påföljdsavgift kan på de grunder som anges i lagen i undantagsfall ges en offentlig varning, om den gärning som strider mot lagen exempelvis kan anses vara ringa.

Bestämmelser om maximibeloppet av den påföljdsavgift som påförs juridiska och fysiska personer finns i 41 § i lagen om Finansinspektionen. I 41 a § finns dessutom flera specialbestämmelser om påföljdsavgiftens maximibelopp. I fråga om försummelser eller överträdelser av skyldigheterna enligt EU:s DORA-förordning föreslås inga särskilda bestämmelser om påföljdavgifternas maximibelopp, utan i dessa fall tillämpas de allmänna bestämmelserna om maximibeloppet i 41 §. I fråga om försummelser eller överträdelser av skyldigheterna enligt EU:s DORA-förordning ska också bestämmelserna i 40 § 3 mom. och 42 § 3 mom. om förhållandet mellan administrativa påföljder och straffrättsliga påföljder tillämpas. Genom dessa bestämmelser säkerställs det att förbudet mot dubbel straffbarhet iakttas. Påföljdsavgift får inte påföras en fysisk person för en gärning eller försummelse som är straffbar enligt lag, utom om gärningen eller försummelsen som helhet betraktad är ringa. Påföljdsavgift får inte påföras en person som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som behandlas i domstol eller den som har dömts för samma gärning genom en lagakraftvunnen dom.

41 §. *Påförande av påföljdsavgift.* I *2 mom*. anges det vilka omständigheter som ska beaktas vid bedömningen av påföljdsavgiftens belopp. Artikel 51.2 i EU:s DORA-förordning innehåller direkt tillämpliga bestämmelser om de omständigheter som den behöriga myndigheten ska ta hänsyn till när den fastställer administrativa sanktioner på grund av en överträdelse av förordningen. Till *3 mom*. fogas därför en förtydligande bestämmelse om att artikel 51.2 i EU:s

DORA-förordning ska iakttas i stället för 2 mom. vid bedömningen av påföljdsavgiftens belopp, om det är fråga om en överträdelse av den förordningen.

43 §. *Offentliggörande av administrativa påföljder och andra beslut.* I artikel 54 i EU:s DORA-förordning finns direkt tillämpliga bestämmelser om offentliggörande av administrativa sanktioner i fall av överträdelser av förordningen. Till paragrafen fogas *ett nytt 5 mom*. enligt vilken artikel 54 i EU:s DORA-förordning ska tillämpas i stället för denna paragraf på offentliggörandet av ett beslut om påförande av en administrativ påföljd, om det är fråga om överträdelse av EU:s DORA-förordning.

50 p §. *Behörig myndighet enligt EU:s DORA-förordning, NIS 2-direktivet och CER-direktivet*
I paragrafen föreskrivs det för närvarande att Finansinspektionen är behörig myndighet enligt artikel 8.1 i direktivet om nät- och informationssäkerhet när det gäller sektorerna 3 och 4 i bilaga II till direktivet. I och med den nya EU-lagstiftningen och upphävandet av direktivet om nät- och informationssäkerhet föreslås det att paragrafen ändras. Enligt det föreslagna *1 mom*. ska Finansinspektionen vara den behöriga myndighet som avses i artikel 46 i EU:s DORA-förordning. Finansinspektionen ska således övervaka efterlevnaden av bestämmelserna i EU:s DORA-förordning och ha tillgång till de tillsyns-, utrednings- och sanktionsbefogenheter som nämns i förordningen på det sätt som föreskrivs i lagen. Finansinspektionen ska också delta i det myndighetssamarbete som avses i förordningen. Dessutom ska Finansinspektionen vara den myndighet som avses i artikel 26.9 i EU:s DORA-förordning, det vill säga ansvara för uppgifter som rör hotbildsstyrd penetrationstestning på nationell nivå. Förslaget påverkar dock inte Finlands Banks verksamhet som ansvarig myndighet för upprätthållandet av verksamhetsmodellen TIBER-FI, som används vid hotbildsstyrd penetrationstestning.

Det föreslagna *2 mom*. motsvarar till sitt innehåll den gällande paragrafen. I momentet föreskrivs det att Finansinspektionen är den behöriga myndighet som avses i artikel 8.1 i NIS 2-direktivet i fråga om sektorerna 3 och 4 i bilaga I i direktivet. Enligt artikeln ska varje medlemsstat utse en eller flera myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VII i direktivet. I Finland finns flera sådana kreditinstitut som definieras i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 samt en sådan operatör av handelsplatser som definieras i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU. Däremot finns det i Finland inga sådana centrala motparter som definieras i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012. Som det konstateras ovan tillämpas de bestämmelser i NIS 2-direktivet som gäller hanteringen av cybersäkerhetsrisker och rapporteringsskyldigheter samt tillsyn och efterlevnadskontroll dock inte på sådana finansiella aktörer som omfattas av tillämpningsområdet för EU:s DORA-förordning. Funktionen som behörig myndighet enligt det föreslagna momentet inbegriper således i praktiken behövligt myndighetssamarbete och informationsutbyte med andra myndigheter enligt NIS 2-direktivet. Den nationella strategin för cybersäkerhet och de nationella ramarna för hantering av cybersäkerhetskriser enligt NIS 2-direktivet samt det europeiska kontaktnätverket för cyberkriser, EU-CyCLONe, ska också omfatta de finanssektorer på vilka direktivet tillämpas.

I *3 mom*. föreslås bestämmelser om Finansinspektionen uppgift att vara den behöriga myndighet som avses i artikel 9.1 i CER-direktivet när det gäller sektorerna 3 (bankverksamhet) och 4 (finansmarknadsinfrastruktur) i bilagan till direktivet. De behöriga myndigheterna enligt EU:s DORA-förordning är i regel behöriga myndigheter i fråga om kritiska aktörer inom sektorerna 3 och 4. Medlemsstaterna ska särskilt identifiera de kritiska aktörerna inom de sektorer som avses i bilagan. Skyldigheterna enligt CER-direktivet tillämpas inte på finansiella aktörer som omfattas av EU:s DORA-förordnings tillämpningsområde, men bankverksamhet och finansmarknadsinfrastruktur beaktas i den strategi för kritiska entiteters motståndskraft och de

riskbedömningar av medlemsstaterna som avses i kapitel II i direktivet. Den nämnda strategin och riskbedömningen och fastställandet av kritiska aktörer inverkar på hur Finansinspektionen dimensionerar och riktar sin tillsynsverksamhet. Till Finansinspektionens uppgifter enligt CER-direktivet hör att i enlighet med artikel 10 i direktivet stödja kritiska aktörer för att stärka deras motståndskraft samt att samarbeta och utbyta information och god praxis med kritiska aktörer. Finansinspektionen ska vara skyldig att samarbeta vid skötseln av sina uppgifter enligt direktivet, vilket det föreskrivs närmare om i 3 f § 4 mom. i lagförslaget.

52 a §. *Samarbete och utbyte av information vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet.* Det föreslås att bestämmelsen upphävs. Bestämmelser om samarbete för att främja cybersäkerheten ska i fortsättningen ingå i den föreslagna nya 3 f §.

71 §. *Rätt och skyldighet att lämna ut information.* I paragrafen ingår de bestämmelser som ger Finansinspektionen rätt att trots sekretessbestämmelserna lämna ut information till andra myndigheter. Till *1 mom*. fogas *en ny 20 punkt* enligt vilken Finansinspektionen har rätt att lämna ut information om störningar och hot relaterade till informations-och kommunikationsteknik till Transport- och kommunikationsverket för genomförande av det samarbete som avses i 3 f § 3 mom. I 1 mom. *19 punkten* görs samtidigt en teknisk ändring med anledning av den nya 20 punkten. I den gällande lagen ingår motsvarande bestämmelse i 52 a §, som föreslås bli upphävd. Jämfört med den gällande bestämmelsen preciseras det i paragrafen att rätten att lämna ut information gäller information om störningar och hot relaterade till informations- och kommunikationsteknik. Rätten att lämna ut information preciseras dessutom i *2 mom*., enligt vilket Finansinspektionen har rätt att lämna ut endast den information som var och en av de myndigheter som nämns i 1 mom. behöver för att kunna utföra sina uppgifter. Transport- och kommunikationsverkets Cybersäkerhetscenter ska i Finland vara en sådan gemensam kontaktpunkt och CSIRT-enhet som avses i NIS 2-direktivet. Cybersäkerhetscentret upprätthåller bland annat en lägesbild över den nationella cybersäkerheten. CSIRT-enheten enligt NIS 2-direktivet har bland annat till uppgift att övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå samt samla in information och tillhandahålla tidiga varningar, larm, meddelanden och information om dem. Transport- och kommunikationsverket är också tillsynsmyndighet enligt NIS 2-direktivet inom sitt verksamhetsområde. Artikel 19 i EU:s DORA-förordning innehåller direkt tillämpliga bestämmelser om Finansinspektionens skyldighet att till andra berörda myndigheter lämna närmare information om allvarliga IKT-relaterade incidenter samt om rätten att lämna dessa myndigheter information om betydande cyberhot. För att det ska vara möjligt att skapa en lägesbild över cybersäkerheten är det viktigt att Finansinspektionen kan lämna ut information också om sådana avvikelser som inte i sig är allvarliga på det sätt som avses i EU:s DORA-förordning.

7.2 Kreditinstitutslagen

9 kap. **Riskhantering**

2 §. *Allmänna krav som ska ställas på riskhanteringssystem.* Det föreslås att *1 mom*. ändras så att det beaktar den ändring i artikel 4.2 i DORA-ändringsdirektivet som gäller artikel 74.1 första stycket i kreditinstitutsdirektivet. Till momentet fogas *en ny 4 punkt*, varvid den nuvarande 4 punkten blir 5 punkt. Till ett kreditinstituts förvaltnings- och styrningssystem ska bland annat höra nätverks- och informationssystem enligt EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den.

16 §. *Operativ risk.* Det föreslås att *3 mom*. ändras så att det beaktar den ändring i artikel 4.3 i DORA-ändringsdirektivet som gäller artikel 85.2 i kreditinstitutsdirektivet. Ett kreditinstitut ska ha beredskaps- och affärskontinuitetsplaner. Genom ändringen av direktivet preciseras det att

ovannämnda planer också innefattar kontinuitets-, åtgärds- och återställningsplaner avseende IKT-risker i enlighet med kraven i EU:s DORA-förordning. Det föreslås att det till momentet fogas en hänvisning till artikel 11 i EU:s DORA-förordning, i vilken det föreskrivs om IKT-kontinuitetspolicyer och IKT-kontinuitetsplaner samt om åtgärds- och återställningsplaner avseende IKT.

11 kap. **Tillsyn över kreditinstitut**

2 §. *Tillsynsmyndighetens bedömning.* Det föreslås att det till *2 mom*. fogas *en ny 11 punkt* som beaktar den ändring i artikel 4.4 i DORA-ändringsdirektivet som gäller artikel 97.1 i kreditinstitutsdirektivet. Enligt den nya punkten ska tillsynsmyndigheten i sin bedömning av de risker som kreditinstitutet är exponerat för och av huruvida kreditinstitutet uppfyller kraven i 9 och 10 kap. i lagen och i EU:s tillsynsförordning beakta de risker som framkommer vid testningen av den digitala operativa motståndskraften enligt kapitel IV i EU:s DORA-förordning. I 1 mom. *10 punkten* görs samtidigt en teknisk ändring med anledning av den nya 11 punkten.

7.3 Lagen om investeringstjänster

7 kap. **Organisering av värdepappersföretags verksamhet**

2 §. *Tillförlitlig organisering av verksamheten.* Det föreslås att *3–5 mom*. ändras så att de beaktar den ändring i artikel 6.1 i DORA-ändringsdirektivet som gäller artikel 16.4 och 16.5 i MiFID II-direktivet. Enligt artikeln förutsätter en tillförlitlig organisering av ett värdepappersföretags verksamhet i fortsättningen att EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den iakttas, inbegripet skydd och autentisering vid informationsöverföring i enlighet med kraven i EU:s DORA-förordning. I 3 och 5 mom. föreslås behövliga ändringar till denna del. Det föreslås att 4 mom. ändras så att det motsvarar artikel 16.5 första stycket i MiFID II-direktivet, som ändrats genom DORA-ändringsdirektivet och som inte längre innehåller något omnämnande av effektiva kontroll- och skyddssystem för informationsbehandlingssystem.

7 a kap. **Algoritmisk handel och direkt elektroniskt tillträde till en handelsplats**

1 §. *Algoritmisk handel.* Det föreslås att *1 mom. 1 punkten* och *2 mom*. ändras så att de beaktar den ändring i artikel 6.2 i DORA-ändringsdirektivet som gäller artikel 17.1 i MiFID II-direktivet. Enligt förslagen ska ett värdepappersföretag som bedriver algoritmisk handel ha inrättat effektiva system och riskkontroller för att säkerställa att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet i enlighet med kraven i EU:s DORA-förordning. Ett sådant värdepappersföretag ska dessutom ha en sådan IKT-kontinuitetspolicy och sådana IKT-kontinuitetsplaner samt sådana åtgärds- och återställningsplaner avseende IKT som avses i artikel 11 i EU:s DORA-förordning och det ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller de krav som föreskrivs i förordningen och med stöd av den.

7.4 Lagen om betalningsinstitut

19 a §. *Hantering av operativa risker och säkerhetsrisker.* I den gällande paragrafen föreskrivs det om riskhanteringsskyldigheter som gäller betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § i lagen om betalningsinstitut och sådana leverantörer av kontoinformationstjänster som avses i 7 b § i lagen om betalningsinstitut. Paragrafen tillämpas dessutom med stöd av hänvisningsbestämmelsen i 9 kap. 16 § 4 mom. i

kreditinstitutslagen på kreditinstitut. Dessa aktörer omfattas av tillämpningsområdet för EU:s DORA-förordning. Det föreslås att *1 mom*. ändras så att det beaktar den ändring i artikel 7.4 i DORA-ändringsdirektivet som gäller artikel 95.1 i betaltjänstdirektivet. Till momentet fogas en informativ bestämmelse som motsvarar den nämnda punkten i direktivet och enligt vilken bestämmelserna i momentet inte begränsar tillämpningen av kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det.

19 b §. *Anmälan om incidenter och bedrägerier.* I den gällande paragrafen föreskrivs det om skyldigheter att anmäla incidenter och bedrägerier. Paragrafen tillämpas på samma aktörer som 19 a §. Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 7.5 i DORA-ändringsdirektivet som gäller artikel 96 i betaltjänstdirektivet. Med stöd av paragrafen ska punkterna 1–5 i artikeln, som har genomförts genom 1 och 3 mom. i den gällande paragrafen, i fortsättningen inte längre tillämpas på ovannämnda aktörer. Därför föreslås det att dessa bestämmelser stryks i lagen.

Paragrafens *1 mom*. motsvarar 2 mom. i den gällande paragrafen. Genom denna bestämmelse har artikel 68.6 i betaltjänstdirektivet genomförts. Den artikeln har inte ändrats genom DORA-ändringsdirektivet. Paragrafens *2 mom*. motsvarar 4 mom. i den gällande paragrafen. Genom denna bestämmelse har artikel 96.6 i betaltjänstdirektivet genomförts. Den artikeln har inte heller ändrats genom DORA-ändringsdirektivet. Paragrafens *3 mom*. motsvarar 5 mom. i den gällande paragrafen.

Paragrafens *4 mom*. innehåller en informativ hänvisning till EU:s DORA-förordnings bestämmelser om rapportering av incidenter. Bestämmelser om skyldigheten för betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 §, sådana leverantörer av kontoinformationstjänster som avses i 7 b § och utgivare av elektroniska pengar att anmäla incidenter relaterade till informations- och kommunikationsteknik samt betalningsrelaterade operativa incidenter eller säkerhetsincidenter finns i kapitel III i EU:s DORA-förordning.

7.5 Lagen om handel med finansiella instrument

3 kap. **Organisering av verksamheten på en reglerad marknad**

1 §. *Krav som gäller organisering av verksamheten på en reglerad marknad*. Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 6.3 och 6.4 a i DORA-ändringsdirektivet som gäller artikel 47 och artikel 48.6 i MiFID II-direktivet. Genom ändringsdirektivet har artikel 47.1 b i MiFID II-direktivet ändrats, artikel 47.1 c upphävts och artikel 48.1 ändrats.

I *1 mom*. i den gällande paragrafen föreskrivs det om organisering av verksamheten på en reglerad marknad, inklusive riskhantering. Momentet kompletteras på det sätt som förutsätts i artikel 6.3 i DORA-ändringsdirektivet med ett krav på hantering av IKT-relaterade risker i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det.

I det gällande 3 mom. föreskrivs det om motståndskraften hos börsens handelssystem i enlighet med artikel 47.1 c och 48.1 i MiFID II-direktivet. Det föreslås att *3 mom*. ändras så att det överensstämmer med den nya ordalydelsen i direktivet. En reglerad marknad ska upprätthålla sin operativa motståndskraft i enlighet med kraven i kapitel II i EU:s DORA-förordning och ha effektiva arrangemang för driftskontinuitet, inklusive en sådan IKT-kontinuitetspolicy och sådana IKT-kontinuitetsplaner samt sådana åtgärds- och återställningsplaner avseende IKT som

upprättats i enlighet med i artikel 11 i EU:s DORA-förordning. Begreppet operativ motståndskraft har tagits in i artikel 48.1 i MiFID II-direktivet genom DORA-ändringsdirektivet. I enlighet med ordalydelsen i direktivet hänför sig den operativa motståndskraften i detta sammanhang till iakttagandet av kraven i kapitel II i EU:s DORA-förordning, och avsikten är inte att i övrigt utvidga en börs lagstadgade skyldigheter.

Enligt *5 mom*. i den gällande paragrafen tillämpas riskhanteringsskyldigheterna enligt 1 mom. på motsvarande sätt på börsers holdingföretag, det vill säga företag som har ett sådant bestämmande inflytande i en börs som avses i 2 kap. 4 § i värdepappersmarknadslagen (746/2012). I momentet behöver det förtydligas att bestämmelsen inte gäller skyldigheten att hantera IKT-relaterade risker i enlighet med EU:s DORA-förordning.

18 §. *Algoritmisk handel.* Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 6.4 a i DORA-ändringsdirektivet som gäller artikel 48.6 i MiFID II-direktivet. Den skyldigheten som ingår i börsens system och förfaranden och som ålägger handelsparter att testa sina algoritmer i börsens testmiljö ska fullgöras i enlighet med kapitel II och IV i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av dem.

7.6 Lagen om placeringsfonder

5 kap. **Soliditet och riskhantering**

1 §. *Fondbolags riskhantering.* Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 1 i DORA-ändringsdirektivet som gäller artikel 12.1 andra stycket led a i MiFID II-direktivet. I direktivet togs det in en hänvisning till de nätverks- och informationssystem som inrättas och förvaltas i enlighet med EU:s DORA-förordning. Som en del av fondbolags riskhantering ska kontroll- och säkerhetsarrangemangen för elektronisk databehandling i fortsättningen överensstämma med EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den.

7.7 Lagen om förvaltare av alternativa investeringsfonder

7 kap. **Organisering av verksamheten**

2 §. *Rutiner för administration och kontroll.* Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 3 i DORA-ändringsdirektivet som gäller artikel 18 i AIFM-direktivet. Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska i fortsättningen överensstämma med EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den.

7.8 Lagen om tilläggspensionsstiftelser och tilläggspensionskassor

1 kap. **Tillämpning av lagen och de centrala principerna för verksamheten**

13 §. *Bestämmelser vars tillämpning beror på antalet försäkrade.* Det föreslås att *1 mom*. ändras så att det nya 4 mom. som fogas till 3 kap. 12 § också ska tillämpas på tilläggspensionsanstalter med färre än 100 försäkrade. Den förenklade IKT-riskhanteringsramen enligt EU:s DORA-förordning lämpar sig för tilläggspensionsanstalter med fler än 15, men färre än 100 försäkrade.

Det föreslås att *2 mom*. ändras så att det nya 4 mom. som fogas till 3 kap. 12 § inte tillämpas på tilläggspensionsanstalter med färre än 16 försäkrade. Enligt artikel 2.3 i EU:s DORA-förordning tillämpas förordningen inte på sådana tilläggspensionsanstalter.

3 kap. **Ledningen och företagsstyrningssystemet**

12 §. *Riktlinjer, system för internkontroll och beredskapsplan.* Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 8 i DORA-ändringsdirektivet som gäller artikel 21.5 i direktiv (EU) 2016/2341.

7.9 Försäkringsbolagslagen

6 kap. **Försäkringsbolagets ledning, företagsstyrningssystem och placering av tillgångar**

8 §. *Allmänna krav på företagsstyrningen.* Det föreslås att paragrafen ändras så att den beaktar den ändring i artikel 2 i DORA-ändringsdirektivet som gäller artikel 41.4 i Solvens II-direktivet.

7.10 Lagen om aktiebolaget Fonden för industriellt samarbete Ab

1 §. Det föreslås att det till paragrafen fogas *ett nytt 5 mom*. enligt vilket EU:s DORA-förordning inte ska tillämpas på Fonden för industriellt samarbete Ab. Genom ändringen utnyttjas i fråga om bolaget optionen i artikel 2.4 i EU:s DORA-förordning, enligt vilken medlemsstaterna från tillämpningsområdet för förordningen får utesluta sådana enheter som avses i artikel 2.5.4–2.5.23 i kreditinstitutsdirektivet, om de är belägna inom deras respektive territorier. Finansinspektionen är den behöriga myndighet som avses i EU:s DORA-förordning, och för närvarande utövar Finansinspektion inte tillsyn över Fonden för industriellt samarbete Ab. Om medlemsstatsoptionen inte utnyttjas, bör det i detta sammanhang föreskrivas om Finansinspektionens uppgift att övervaka att skyldigheterna enligt EU:s DORA-förordning fullgörs i fråga om bolaget samt om behövliga tillsynsbefogenheter och tillsynsavgifter i anslutning till detta. Det kan inte anses ändamålsenligt att skapa separata tillsynsarrangemang i fråga om en enskild författning, utan styrningen och tillsynen bör bedömas som en helhet i samband med att lagstiftningen om bolaget revideras. Därför är det motiverat att utnyttja medlemsstatsoptionen enligt EU:s DORA-förordning för bolagets del.

7.11 Lagen om statens specialfinansieringsbolag

3 §. *Förvaltning*. Till paragrafen fogas *ett nytt 5 mom*. enligt vilket EU:s DORA-förordning inte ska tillämpas på Finnvera Abp. Genom ändringen utnyttjas optionen enligt artikel 2.4 i EU:s DORA-förordning i fråga om Finnvera Abp på motsvarande grunder som de som konstaterats ovan i fråga om Fonden för industriellt samarbete Ab.

8 Bestämmelser på lägre nivå än lag

Genomförandet av artikel 5 i DORA-ändringsdirektivet förutsätter ändringar i följande förordningar: finansministeriets förordning om de uppgifter som ska lämnas in för upprättandet av kreditinstituts och värdepappersföretags resolutionsplaner och ingå i dem (1284/2014), finansministeriets förordning om omständigheter som ska beaktas vid bedömning av ett kreditinstituts och värdepappersföretags eller en koncerns avvecklings- och omorganiseringsmöjligheter (1285/2014), finansministeriets förordning om uppgifter som ska framgå av ett kreditinstituts och värdepappersföretags återhämtningsplaner (1286/2014). Ändringsbehoven beror på de ovan beskrivna ändringarna i resolutionsdirektivet, som beaktar den digitala operativa motståndskraften och EU:s DORA-förordning i kraven på innehållet i kreditinstitutens och värdepappersföretagens återhämtnings- och resolutionsplaner samt i de krav som gäller bedömning av möjligheterna till resolution och omstrukturering.

Dessutom förutsätter genomförandet av artikel 7.2 i DORA-ändringsdirektivet ändringar i finansministeriets förordning om utredningar som ska fogas till ansökan om auktorisation för betalningsinstitut (1040/2017).

9 Ikraftträdande

Lagarna föreslås träda i kraft i den 17 januari 2025.

10 Samband med andra propositioner

I regeringens proposition till riksdagen med förslag till lag om leverantörer av kryptotillgångstjänster och om marknader för kryptotillgångar samt till vissa andra lagar (RP 31/2024 rd) föreslås liksom i denna proposition ändringar i 5, 38 och 41 § i lagen om Finansinspektionen. En ändring av 5 § i lagen om Finansinspektionen föreslås också i regeringens proposition till riksdagen med förslag till lag om ändring av lagen om Keva och till vissa lagar som har samband med den (RP 55–/2024 rd). Till den delen ska ändringarna samordnas i samband med att propositionerna behandlas i riksdagen.

11 Förhållande till grundlagen samt lagstiftningsordning

11.1 Tillsynsbefogenheter som gäller tredjepartsleverantörer av IKT-tjänster

Enligt 18 § 1 mom. i Finlands grundlag har var och en i enlighet med lag rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt.

Finansmarknadslagstiftningen och Finansinspektionens relaterade tillsynsbefogenheter innebär inskränkningar av näringsfriheten. Den gällande lagen om Finansinspektionen har i behövliga delar satts i kraft med grundlagsutskottets medverkan.

I regeringens proposition föreslås inga nya typer av befogenheter för Finansinspektionen och inte heller i övrigt föreslås några ändringar i de grundläggande premisserna för lagstiftningen. Genom det första lagförslaget i propositionen läggs tredjepartsleverantörer av IKT-tjänster enligt EU:s DORA-förordning till förteckningen över andra finansmarknadsaktörer. På det sättet utsträcks Finansinspektionens tillsynsbefogenheter till att omfatta tredjepartsleverantörer av IKT-tjänster. Tillsynsbefogenheterna får utnyttjas när det behövs för att Finansinspektionen ska kunna utföra sina lagstadgade uppgifter. Finansinspektionens rätt enligt 18 § i lagen om Finansinspektionen att få uppgifter av tillsynsobjekt och andra finansmarknadsaktörer samt Finansinspektionens granskningsrätt enligt 24 § gäller redan för närvarande företag som på uppdrag av tillsynsobjekt eller andra finansmarknadsaktörer sköter uppgifter i anslutning till dessas datasystem. Ändringen är alltså inte betydande i sak, även om Finansinspektionens tillsynsbefogenheter utvidgas i viss mån i förhållande till dessa företag. Ändringen grundar sig på villkoret i EU:s DORA-förordning att Finansinspektionen ska ha alla befogenheter som behövs för att den ska kunna utföra sina uppgifter enligt förordningen.

De föreslagna befogenheterna är relevanta för näringsfriheten och rätten att fritt utöva ett yrke enligt 18 § 1 mom. i grundlagen. Grundlagsutskottet har inte ansett att sådana befogenheter är problematiska ur konstitutionell synvinkel (till exempel GrUU 67/2002 rd och GrUU 28/2008 rd).

11.2 Administrativa påföljder

Enligt 21 § i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring samt andra garantier för en rättvis rättegång och god förvaltning ska tryggas genom lag.

Det föreslås att bestämmelserna om administrativa påföljder i lagen om Finansinspektionen kompletteras med anledning av EU:s DORA-förordning. EU:s DORA-förordning förutsätter att medlemsstaterna sätter i kraft lämpliga effektiva, proportionella och avskräckande administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen. Finansinspektionen ska enligt förslaget kunna påföra den som försummar eller bryter mot sina skyldigheter enligt EU:s DORA-förordning en påföljdsavgift. Den som försummar eller bryter mot skyldigheten att ha en förenklad IKT-riskhanteringsram enligt förordningen ska kunna påföras en ordningsavgift.

Grundlagsutskottets vedertagna tolkning är att sådana påföljdsavgifter med avseende på 81 § i grundlagen varken är skatter eller avgifter, utan administrativa påföljder av sanktionskaraktär för en lagstridig gärning. I sak jämställer utskottet en ekonomisk påföljd av straffkaraktär med en straffrättslig påföljd (GrUU 14/2013 rd, GrUU 17/2012 rd, GrUU 9/2012 rd, s. 2, GrUU 55/2005 rd, s. 2, och GrUU 32/2005 rd, s. 2). De allmänna grunderna för administrativa påföljder ska bestämmas i lag på det sätt som grundlagens 2 § 3 mom. förutsätter, eftersom det innebär utövning av offentlig makt att påföra en sådan avgift. Grundlagsutskottet har också ansett att det är fråga om betydande utövning av offentlig makt.

Lagen måste exakt och tydligt föreskriva om grunderna för betalningsskyldigheten och avgiftens storlek, rättsskyddet för den betalningsskyldige och grunderna för verkställigheten av lagen (GrUU 14/2013 rd, GrUU 17/2012 rd, GrUU 9/2012 rd, s. 2, GrUU 57/2010 rd, s. 2, GrUU 55/2005 rd, s. 2, och GrUU 32/2005 rd, s. 2). Även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen i grundlagens 8 § inte direkt gäller regleringen av administrativa påföljder, kan det allmänna kravet på exakthet ändå inte förbigås i en reglering av detta slag (GrUU 14/2013 rd, GrUU 17/2012 rd, GrUU 9/2012 rd, s. 2, GrUU 57/2010 rd, s. 2 och GrUU 74/2002 rd, s. 5). Dessutom ska bestämmelserna uppfylla kraven i fråga om rätt proportion på sanktionerna (GrUU 28/2014 rd, GrUU 15/2014 rd). I fråga om administrativa sanktioner bör det också noteras att förfarandet för dem inte får stå i strid med oskyldighetspresumtionen i grundlagens 21 § och inte heller får bygga uteslutande på omvänd bevisbörda eller strikt objektivt ansvar (se även GrUU 32/2005 rd, s. 3 och GrUU 4/2004 rd, s. 7).

De bestämmelser om administrativa påföljder som ingår i det första lagförslaget i propositionen motsvarar till sin karaktär de bestämmelser som redan finns i den gällande lagstiftningen och som utfärdats med grundlagsutskottets medverkan (GrUU 17/2012 rd, GrUU 15/2016 rd och GrUU 43/2013 rd). I bestämmelserna om ordningsavgift och påföljdsavgift i lagen om Finansinspektionen förtecknas de bestämmelser som när de försummas eller överträds kan leda till att påföljden påförs. Dessa bestämmelser kompletteras så att en påföljd kan påföras den som försummar eller bryter mot de relevanta bestämmelserna i EU:s DORA-förordning. Det föreslås inga ändringar i de övriga villkoren eller i förfarandet för påförande av ordningsavgift och påföljdsavgift.

Utan uttryckliga bestämmelser kan Finansinspektionen inte påföra någon annan administrativ påföljd än offentlig varning enligt 39 § i lagen om Finansinspektionen. Om inga närmare bestämmelser införs om brott mot eller försummelser av skyldigheterna enligt EU:s DORA-förordning kan Finansinspektionen alltså endast ge en offentlig varning för en överträdelse eller försummelse, men inte påföra några administrativa påföljder som eurobelopp. Det innebär att Finansinspektionen inte nödvändigtvis kan ingripa effektivt i eventuella överträdelser.

I bestämmelserna om administrativa påföljder i lagen om Finansinspektionen beaktas dels påföljdernas exakthet och proportionalitet, dels flexibiliteten och den avskräckande effekten vid tillämpningen av påföljder. Finansinspektionen ska ha flexibla möjligheter att i varje enskilt fall av brott mot eller försummelse av lagstiftningen påföra den mest ändamålsenliga påföljden med hänsyn till de rådande omständigheterna. Administrativa påföljder enligt den lagen gör det möjligt att snabbt och effektivt ingripa i förfaranden som strider mot finansmarknadslagstiftningen, vilket effektiviserar den offentliga tillsynen över finansmarknaden. Med tanke på den samhälleliga vikten av regleringen om den digitala operativa motståndskraften i finanssektorn och finansmarknadstillsynens trovärdighet är det viktigt att Finansinspektionen har tillgång till effektiva sanktioner i fall där någon bryter mot eller försummar skyldigheterna enligt EU:s DORA-förordning. Därför är det motiverat att i dessa fall påföra en påföljdsavgift. Samtidigt måste man beakta de administrativa påföljdernas proportionalitet. Bestämmelserna om påförande av administrativa påföljder möjliggör också i övrigt prövningsmarginal efter behov för Finansinspektionen. Enligt artikel 51.2 i EU:s DORA-förordning ska man när man fastställer en administrativ sanktion ta hänsyn till i vilken utsträckning överträdelsen är avsiktlig eller beror på försummelse och till alla andra relevanta omständigheter, bland annat överträdelsens väsentlighet, svårighetsgrad och varaktighet. När man bedömer om skyldigheterna enligt EU:s DORA-förordning följs ska man i enlighet med proportionalitetsprincipen i artikel 4 i förordningen också ta hänsyn till bland annat den finansiella entitetens storlek och ekonomiska ställning. Bedömningen av proportionaliteten hos en administrativ påföljd gäller inte endast dimensioneringen av påföljdsavgiften, utan också valet av påföljdsslag. Enligt 42 § i lagen kan Finansinspektionen omvandla en påföljdsavgift till en offentlig varning eller avstå från att påföra påföljdsavgift om överträdelsen är obetydlig. I artikel 16 i EU:s DORA-förordning föreskrivs det om krav på en förenklad IKT-riskhanteringsram som tillämpas på vissa mindre aktörer. I princip räcker det med en lindrigare påföljd, det vill säga ordningsavgift, vid brott mot eller försummelse av dessa krav.

11.3 Rätt att lämna ut sekretessbelagda uppgifter

Enligt 10 § 1 mom. i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Bestämmelsen i 71 § 1 mom. 20 punkten i lagen om Finansinspektionen om rätten att lämna ut information trots sekretessbestämmelserna är relevant med tanke på skyddet för privatlivet och personuppgifter. Grundlagsutskottet har bedömt bestämmelser om myndigheternas rätt att trots sekretesskyldigheten få och lämna ut information med avseende på skyddet för privatliv och personuppgifter i 10 § 1 mom. i grundlagen och då noterat bland annat vad och vem rätten att få information gäller och hur rätten är kopplad till nödvändighetskriteriet (se t.ex. GrUU 15/2018 rd). Myndigheternas rätt att få och möjlighet att lämna ut uppgifter har kunnat gälla ”behövliga uppgifter” för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att "uppgifterna är nödvändiga" för ett visst syfte (se t.ex. GrUU 17/2016 rd, s. 5). Vid bedömningen av exakthet och innehåll har utskottet fäst särskild vikt vid huruvida de uppgifter som ska lämnas ut är känsliga uppgifter. Om de föreslagna bestämmelserna om utlämnande av information också hänfört sig till känsliga uppgifter har ett villkor för tillämpning av vanlig lagstiftningsordning varit att bestämmelserna preciserats så att

de följer grundlagsutskottets återgivna praxis för bestämmelser som rör rätten att få och lämna ut myndighetsuppgifter trots sekretess (GrUU 38/2016 rd, s. 3). Å andra sidan har utskottet ansett att grundlagen inte tillåter en mycket vag och ospecificerad rätt att få uppgifter, låt vara att den är knuten till nödvändighetskriteriet (se t.ex. GrUU 71/2014 rd, s. 3/I, GrUU 62/2010 rd, s. 4/I och GrUU 59/2010 rd, s. 4/I).

Grundlagsutskottet anser att dataskyddsförordningens detaljerade bestämmelser, som tolkas och tillämpas i enlighet med de rättigheter som garanteras i EU:s stadga om de grundläggande rättigheterna, allmänt taget utgör en tillräcklig rättslig grund även med avseende på skyddet för privatlivet och personuppgifter enligt 10 § i grundlagen. Skyddet för personuppgifter bör i första hand tillgodoses utifrån den allmänna dataskyddsförordningen och den allmänna lagstiftningen på nationell nivå (se t.ex. GrUU 92/2022 rd). Bestämmelsen om utlämnande av information i 71 § i det första lagförslaget i regeringens proposition gäller uppgifter om störningar relaterade till informations- och kommunikationsteknik, och eventuell sekretess för sådana uppgifter grundar sig i princip på de finansiella bolagens företagshemligheter. Utlämnandet av information kan inte anses vara förknippat med några särskilda risker som gäller skyddet för personuppgifter. Den information som lämnas ut med stöd av bestämmelsen innehåller allmänt taget endast i begränsad omfattning personuppgifter, eftersom det är fråga om information om affärsverksamhet.

Regeringen anser att de föreslagna lagarna kan behandlas i vanlig lagstiftningsordning.

Kläm

Eftersom förordningen om cybersäkerhet och operativ motståndskraft inom finanssektorn innehåller bestämmelser som enligt förslaget ska kompletteras genom lag, och de relevanta direktiven innehåller bestämmelser som enligt förslaget ska genomföras genom lag, föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av lagen om Finansinspektionen

I enlighet med riksdagens beslut

upphävs i lagen om Finansinspektionen (878/2008) 52 a §, sådan den lyder i lag 959/2018,

ändras 5 § 40 punkten, 38 § 1 mom. 11 punkten, 40 § 2 mom. 11 och 12 punkten, 41 § 3 mom., 50 p § och 71 § 1 mom. 19 punkten,

sådana de lyder, 5 § 40 punkten och 38 § 1 mom. 11 punkten i lag 184/2023, 40 § 2 mom. 11 och 12 punkten i lag 214/2022, 41 § 3 mom. i lag 205/2022, 50 p § i lag 291/2018 och 71 § 1 mom. 19 punkten i lag 524/2021, samt

fogas till 3 § 2 mom., sådant det lyder delvis ändrat i lagarna 1198/2014, 1145/2015, 1442/2016, 445/2023 och 1261/2023, nya 7 och 7 a-punkter i stället för de 7 och 7 a-punkter som upphävts genom lag 1442/2016, till lagen en ny 3 f §, till 5 §, sådan den lyder i lagarna 752/2012, 902/2012, 254/2013, 170/2014, 198/2015, 520/2016, 737/2016, 1442/2016, 228/2017, 575/2017, 893/2017, 1071/2017, 241/2018, 1229/2018, 215/2019, 296/2019, 517/2019, 574/2019, 963/2019, 316/2020, 524/2021, 599/2021, 205/2022, 184/2023 och 192/2023, en ny 41 punkt, till 38 § 1 mom., sådant det lyder i lagarna 752/2012, 254/2013, 1198/2014, 1055/2016, 893/2017, 316/2020, 379/2021, 153/2022, 205/2022 och 184/2023, en ny 12 punkt, till 38 §, sådan den lyder i lagarna 752/2012, 254/2013, 611/2014, 1198/2014, 1055/2016, 893/2017, 316/2020, 379/2021, 153/2022, 205/2022 och 184/2023, ett nytt 7 mom., till 40 § 2 mom., sådant det lyder i lagarna 1071/2017, 1108/2018, 316/2020, 379/2021, 599/2021, 941/2021 och 214/2022, en ny 13 punkt, till 43 §, sådan den lyder i lagarna 176/2016, 1071/2017 och 524/2021, ett nytt 5 mom. och till 71 § 1 mom., sådant det lyder delvis ändrat i lagarna 752/2012, 611/2014, 651/2014, 1198/2014, 505/2015, 520/2016, 1442/2016, 446/2017, 1071/2017, 402/2018, 574/2019, 569/2020, 270/2021 och 524/2021, en ny 20 punkt som följer:

3 §

Uppgifter

— —

Finansinspektionen fullgör sina lagstadgade uppgifter genom att

— —

7) främja cybersäkra tillvägagångssätt hos finansmarknadsaktörer,

7 a) främja kritiska finansmarknadsaktörers motståndskraft,

— —

3 f §

Myndighetssamarbete för att främja cybersäkerhet och motståndskraft

Finansinspektionen samarbetar med finansministeriet, social- och hälsovårdsministeriet, Finlands Bank, Verket för finansiell stabilitet, Transport- och kommunikationsverket och andra behöriga myndigheter för att hantera störningar relaterade till informations- och kommunikationsteknik (*IKT*) och för att minska konsekvenserna av sådana störningar.

Finansinspektionen deltar i myndighetssamarbete enligt artiklarna 32 och 47–49 i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan *EU:s DORA-förordning*, och i verksamheten inom det europeiska ramverket för samordning av åtgärder mot systemiska cyberincidenter samt samarbetar också i övrigt med Europeiska centralbanken, Europeiska systemrisknämnden, Europeiska unionens cybersäkerhetsbyrå, de europeiska tillsynsmyndigheterna, andra EU-myndigheter och utländska EES-tillsynsmyndigheter för att hantera störningar relaterade till informations-och kommunikationsteknik och för att minska konsekvenserna av sådana störningar.

Finansinspektionen ska samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (*NIS 2-direktivet*).

Finansinspektionen ska samarbeta med finansministeriet, inrikesministeriet, Försörjningsberedskapscentralen och andra behöriga myndigheter för skötseln av uppgifter enligt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, nedan *CER-direktivet*, för att stärka kritiska aktörers motståndskraft och för att främja frivilligt informationsutbyte mellan dem.

5 §

Andra finansmarknadsaktörer

Med *andra finansmarknadsaktörer* avses i denna lag

— —

40) den som med stöd av 4 § i lagen om registrering av vissa kreditgivare och kreditförmedlare (186/2023) är skyldig att anmäla sig till det register över kreditgivare och förmedlare av person-till-person-lån som förs av Finansinspektionen,

41) sådana tredjepartsleverantörer av IKT-tjänster som avses i artikel 3.19 i EU:s DORA-förordning.

38 §

Ordningsavgift

Finansinspektionen ska ålägga den att betala ordningsavgift som uppsåtligen eller av oaktsamhet

— —

11) försummar eller bryter mot anmälningsskyldigheten enligt 8 § 3 mom. i lagen om registrering av vissa kreditgivare och kreditförmedlare,

12) försummar eller bryter mot skyldigheten att hantera IKT-risker enligt artikel 16 i EU:s DORA-förordning.

— —

Om ordningsavgift påförs med stöd av 1 mom. 12 punkten, ska artikel 51.2 i EU:s DORA-förordning iakttas i stället för 2 mom. i fråga om de omständigheter som ska beaktas vid bedömningen av ordningsavgiftens belopp.

40 §

Påföljdsavgift

— —

Påföljdsavgift ska också påföras den som uppsåtligen eller av oaktsamhet försummar eller bryter mot

— —

11) bestämmelserna i artikel 5 i Europaparlamentets och rådets förordning (EU) 2020/852 om inrättande av en ram för att underlätta hållbara investeringar och om ändring av förordning (EU) 2019/2088, nedan *taxonomiförordningen*, om transparens i fråga om miljömässigt hållbara investeringar i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, bestämmelserna i artikel 6 om transparens i fråga om finansiella produkter som främjar miljörelaterade egenskaper i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, eller bestämmelserna i artikel 7 om transparens i fråga om andra finansiella produkter i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter,

12) bestämmelserna i artiklarna 5–7 i PEPP-förordningen om registreringsskyldighet och bestämmelserna om lämnande av falska eller vilseledande uppgifter som grund för registreringen av en PEPP-produkt i det centrala offentliga register som förs av Europeiska försäkrings- och tjänstepensionsmyndigheten, bestämmelserna i artikel 18 om erbjudande av portabilitetsmöjlighet, bestämmelserna i artikel 19 om användning av underkonton för PEPP-produkter, bestämmelserna i artikel 20 om skyldighet att lämna information i anknytning till öppnande av ett nytt underkonto, bestämmelserna i artikel 21 om information om portabilitet till de behöriga myndigheterna, bestämmelserna i artikel 22 om en allmän princip som gäller PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 23 om distributionsregler för olika typer av PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 24 om elektronisk distribution och om användning av andra varaktiga medier, bestämmelserna i artikel 25 om krav på produkt-övervakning och produktstyrning, bestämmelserna i artikel 26 om PEPP-faktablad, bestämmelserna i artikel 27 om PEPP-faktabladets språk, bestämmelserna i artikel 28 om PEPP-faktabladets innehåll, bestämmelserna i artikel 29 om marknadsföringsmaterial, bestämmelserna i artikel 30 om översyn av PEPP-faktabladet, bestämmelserna i artikel 31 om skadeståndsansvar, bestämmelserna i artikel 32 om PEPP-avtal som täcker biometriska risker, bestämmelserna i artikel 33 om tillhandahållande av PEPP-faktabladet, bestämmelserna i artikel 34 om specifikation av PEPP-kundens krav och behov samt tillhandahållande av rådgivning, bestämmelserna i artikel 35 om allmänna bestämmelser som gäller PEPP-pensionsbesked, bestämmelserna i artikel 36 om innehållet i PEPP-pensionsbeskedet, bestämmelserna i artikel 37 om kompletterande information i PEPP-pensionsbeskedet, bestämmelserna i artikel 38 om information som ska lämnas till PEPP-sparare under tiden före pensionering och till PEPP-förmånstagare under utbetalningsfasen, bestämmelserna i artikel 39 om information som på begäran ska lämnas till PEPP-sparare och PEPP-förmånstagare, bestämmelserna i artikel 40 om allmänna bestämmelser som gäller rapportering till nationella myndigheter, bestämmelserna i artikel 41 om investeringsregler under intjänandefasen, bestämmelserna i artikel 42 om allmänna bestämmelser som gäller PEPP-spararens investeringsalternativ, bestämmelserna i artikel 43 om PEPP-spararens val av investeringsalternativ, bestämmelserna i artikel 44 om villkor för ändring av det valda investeringsalternativet, bestämmelserna i artikel 45 om bas-PEPP-produkten, bestämmelserna i artikel 46 om riskreduceringstekniker, bestämmelserna i artikel 47 om villkor som rör intjänandefasen, bestämmelserna i artikel 48 om förvaringsinstitutets förvarings- och övervakningsuppgifter, bestämmelserna i artikel 50 om hantering av klagomål från PEPP-kunder, bestämmelserna i artikel 52 om tillhandahållande av bytesmöjlighet, bestämmelserna i artikel 53 om inledande av byte, bestämmelserna i artikel 54 om avgifter och kostnader i samband med byte, bestämmelserna i artikel 55 om skydd av PEPP-sparare mot finansiell förlust eller bestämmelserna i artikel 56 om information om bytesmöjligheten,

13) bestämmelserna om hantering av IKT-risker i artiklarna 5–14 i EU:s DORA-förordning, bestämmelserna om hantering av, klassificering av och rapportering om IKT-relaterade incidenter i artiklarna 17–19 i den förordningen, bestämmelserna om testning av digital operativ

motståndskraft i artiklarna 24–27 i den förordningen eller bestämmelserna om hantering av IKT-tredjepartsrisker i artiklarna 28–30 i den förordningen, vilka är förpliktande för i artikel 2.2 i den förordningen avsedda finansiella entiteter.

— —

41 §

Påförande av påföljdsavgift

— —

Om det är fråga om överträdelse av förordningen om referensvärden, ska utöver det som föreskrivs i 2 mom. också förfarandets inverkan på realekonomin beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av Europaparlamentets och rådets förordning (EU) 2017/1129 om prospekt som ska offentliggöras när värdepapper erbjuds till allmänheten eller tas upp till handel på en reglerad marknad, och om upphävande av direktiv 2003/71/EG, nedan *prospektförordningen*, ska överträdelsens inverkan också på icke-professionella kunders ställning beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av EU:s gräsrotsfinansieringsförordning ska överträdelsens inverkan på investerarnas intressen beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av EU:s DORA-förordning, ska artikel 51.2 i den förordningen iakttas i stället för 2 mom. vid bedömningen av påföljdsavgiftens belopp.

— —

43 §

Offentliggörande av administrativa påföljder och andra beslut

— —

Om ordningsavgift, offentlig varning eller påföljdsavgift påförs på grund av en överträdelse av EU:s DORA-förordning, ska artikel 54 i EU:s DORA-förordning tillämpas i stället för denna paragraf på offentliggörandet av beslutet.

50 p §

Behörig myndighet enligt EU:s DORA-förordning, NIS 2-direktivet och CER-direktivet

Finansinspektionen är den behöriga myndighet som avses i artikel 46 i EU:s DORA-förordning och den myndighet som avses i artikel 26.9 i den förordningen.

Finansinspektionen är den behöriga myndighet som avses i artikel 8.1 i NIS 2-direktivet i fråga om sektorerna 3 och 4 i bilaga I till direktivet.

Finansinspektionen är den behöriga myndighet som avses i artikel 9.1 i CER-direktivet i fråga om sektorerna 3 och 4 i bilagan till direktivet.

71 §

Rätt och skyldighet att lämna ut information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Finansinspektionen utan hinder av sekretessbestämmelserna rätt att lämna ut information till

— —

19) Europeiska kommissionen när sådan information i anknytning till tillsynen över finansmarknaden krävs för att kommissionen ska kunna utöva sina befogenheter,
20) Transport- och kommunikationsverket för genomförande av det samarbete som avses i 3 f § 3 mom., när det gäller störningar och hot relaterade till informations- och kommunikationsteknik.

Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 9 och 11 kap. i kreditinstitutslagen

I enlighet med riksdagens beslut
ändras i kreditinstitutslagen (610/2014) 9 kap. 2 § 1 mom. och 16 § 3 mom. samt 11 kap. 2 § 2 mom. 10 punkten,
av dem 11 kap. 2 § 2 mom. 10 punkten sådan den lyder i lag 233/2021, samt
fogas till 11 kap. 2 § 2 mom., sådant det lyder i lag 233/2021, en ny 11 punkt som följer:

9 kap.

Riskhantering

2 §

Allmänna krav som ska ställas på riskhanteringssystem

Ett kreditinstitut ska ha effektiva, tillförlitliga och dokumenterade förvaltnings- och styrningssystem för identifiering, hantering, begränsning, övervakning och rapportering av nuvarande och framtida risker som kreditinstitutet och dess verksamhet exponeras för. Systemen ska omfatta
1) en tydlig organisationsstruktur med väldefinierade och konsekventa befogenhets- och ansvarsförhållanden,
2) effektiva rapporteringsprocesser för riskhanteringen,
3) sunda processer för intern kontroll, inklusive förvaltnings- och redovisningsrutiner,
4) nätverks- och informationssystem enligt Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan *EU:s DORA-förordning*, och de bestämmelser som utfärdats med stöd av den,
5) en ersättningspolicy och ersättningspraxis som är förenlig med och främjar sund och effektiv riskhantering.

---

16 §

Operativ risk

— —

Kreditinstitutet ska ha beredskaps- och kontinuitetsplaner för att bereda sig för allvarliga störningar i affärsverksamheten samt säkerställa sin förmåga att fortlöpande bedriva verksamhet och begränsa förlusterna i störningssituationer. Bestämmelser om den kontinuitetspolicy och de kontinuitetsplaner för informations- och kommunikationstekniken (*IKT*) i kreditinstitutets affärsverksamhet och de åtgärds- och återställningsplaner avseende IKT som ska ingå i de nämnda planerna finns i artikel 11 i EU:s DORA-förordning.

— —

11 kap.

Tillsyn över kreditinstitut

2 §

Tillsynsmyndighetens bedömning

— —

Tillsynsmyndigheten ska i sin bedömning enligt 1 mom. beakta åtminstone

— —

10) den ränterisk i den finansiella balansräkningen som riktar sig mot kreditinstitutet,

11) de risker som framkommer vid testningen av den digitala operativa motståndskraften enligt kapitel IV i EU:s DORA-förordning.

— —

———

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av 7 kap. 2 § och 7 a kap. 1 § i lagen om investeringstjänster

I enlighet med riksdagens beslut

ändras i lagen om investeringstjänster (747/2012) 7 kap. 2 § 3–5 mom. och 7 a kap. 1 § 1 mom. 1 punkten och 2 mom., sådana de lyder i lag 1069/2017, som följer:

7 kap.

Organisering av värdepappersföretags verksamhet

2 §

Tillförlitlig organisering av verksamheten

— —

Värdepappersföretaget ska vidta rimliga åtgärder för att säkerställa kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och bedrivandet av investeringsverksamhet. Värdepappersföretaget ska i det syftet använda ändamålsenliga och proportionella system, resurser och förfaranden. Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan *EU:s DORA-förordning*, och de bestämmelser som utfärdats med stöd av den.

Värdepappersföretaget ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för intern kontroll och effektiva riskbedömningsmetoder.

Värdepappersföretaget ska, utan att begränsa Finansinspektionens tillgång till information, ha inrättat sunda skyddsmekanismer för att garantera skyddet och autentiseringen vid informationsöverföringen i enlighet med EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den, minimera risken för dataförvanskning och för obehörig åtkomst samt förhindra informationsläckor så att uppgifterna alltid behandlas konfidentiellt.

— —

7 a kap.

Algoritmisk handel och direkt elektroniskt tillträde till en handelsplats

1 §

Algoritmisk handel

Ett värdepappersföretag som bedriver algoritmisk handel ska ha inrättat effektiva system och riskkontroller som är anpassade för den verksamhet som drivs för att

1) säkerställa att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det samt att de omfattas av lämpliga handelströsklar och handelslimiter,

— —

Ett värdepappersföretag som avses i 1 mom. ska dessutom ha inrättat effektiva arrangemang för driftskontinuitet för att hantera avbrott av driften i sina handelssystem. Värdepappersföretaget ska ha en sådan kontinuitetspolicy och sådana kontinuitetsplaner för informations- och kommunikationsteknik (*IKT*) samt sådana åtgärds- och återställningsplaner avseende IKT som avses i artikel 11 i EU:s DORA-förordning. Värdepappersföretaget ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller de krav som föreskrivs i 1 och 2 mom. och i EU:s DORA-förordning och med stöd av den.

— —

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av 19 a och 19 b § i lagen om betalningsinstitut

I enlighet med riksdagens beslut

ändras i lagen om betalningsinstitut (297/2010) 19 a § 1 mom. och 19 b §, sådana de lyder i lag 890/2017, som följer:

19 a §

Hantering av operativa risker och säkerhetsrisker

Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska inrätta ett tillräckligt riskhanteringssystem med riskhanteringsåtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker i anslutning till de betaltjänster som de tillhandahåller. De ska ha ett effektivt incidenthanteringsförfarande och kunna upptäcka och klassificera allvarliga operativa incidenter och säkerhetsincidenter. Bestämmelserna i detta moment begränsar inte tillämpningen av kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan *EU:s DORA-förordning*, och de bestämmelser som utfärdats med stöd av det.

— —

19 b §

Anmälan om incidenter och bedrägerier

Ett kontoförande betalningsinstitut och en person som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § ska göra en anmälan till Finansinspektionen, om de upptäcker att en leverantör av kontoinformationstjänster eller en leverantör av betalningsinitieringstjänster använder ett betalkonto på ett obehörigt eller bedrägligt sätt och det kontoförande betalningsinstitutet eller den som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § på denna grund förhindrar leverantörens tillträde till betalkontot. Anmälan ska innehålla tillräcklig information om incidenten och om åtgärder med anledning av den. Finansinspektionen ska bedöma fallet och vidta behövliga åtgärder.

Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska minst en gång per år lämna Finansinspektionen statistiska uppgifter om bedrägerier i samband med betalningsinstrument. Finansinspektionen ska lämna Europeiska bankmyndigheten och Europeiska centralbanken dessa uppgifter i aggregerad form. Finansinspektionen får meddela närmare föreskrifter om den rapporteringsskyldighet som avses i detta moment.

Vad som föreskrivs i 1 och 2 mom. tillämpas inte på institut för elektroniska pengar.

Bestämmelser om skyldigheten för betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 §, sådana leverantörer av kontoinformationstjänster som avses i 7 b § och utgivare av elektroniska pengar att anmäla incidenter relaterade till informations- och kommunikationsteknik samt betalningsrelaterade operativa incidenter eller säkerhetsincidenter finns i kapitel III i EU:s DORA-förordning.

———

Denna lag träder i kraft den 20 .

_____

5.

Lag

om ändring av 3 kap. 1 och 18 § i lagen om handel med finansiella instrument

I enlighet med riksdagens beslut

ändras i lagen om handel med finansiella instrument (1070/2017) 3 kap. 1 § 1, 3 och 5 mom. samt 18 § 1 mom. 1 punkten, sådana de lyder i lag 295/2019, som följer:

3 kap.

Organisering av verksamheten på en reglerad marknad

1 §

Krav som gäller organisering av verksamheten på en reglerad marknad

En börs ska organisera sin verksamhet på ett tillförlitligt sätt med beaktande av arten och omfattningen av dess affärsverksamhet. Börsen ska i alla situationer säkerställa den verksamhetsrelaterade riskhanteringen och verksamhetens kontinuitet. Börsen ska hantera risker relaterade till informations- och kommunikationsteknik (*IKT*) i enlighet med kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan *EU:s DORA-förordning*, och de bestämmelser som utfärdats med stöd av det.

— —

Börsen ska säkerställa tillförlitligheten och kontinuiteten i handelssystemet också i störningssituationer. Börsen ska ha operativ motståndskraft, som den ska upprätthålla i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det, så att börsens handelssystem är tillräckligt motståndskraftiga, att den har tillräcklig kapacitet för att hantera toppbelastning i fråga om order- och meddelandevolymer och att den kan upprätthålla ordnad handel under svåra förhållanden på marknaden. För att säkerställa kontinuiteten i tjänsterna på en reglerad marknad ska börsen ha en sådan IKT-kontinuitetspolicy och sådana IKT-kontinuitetsplaner samt sådana åtgärds- och återställningsplaner avseende IKT som avses i artikel 11 i EU:s DORA-förordning. Börsen ska regelbundet testa handelssystemets funktion med belastningstest för att uppfylla de krav som nämns ovan.

— —

Vad som i 1 mom. föreskrivs om börser ska på motsvarande sätt tillämpas på börsers holdingföretag, med undantag för skyldigheten att hantera IKT-relaterade risker i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det.

— —

18 §

Algoritmisk handel

En börs ska ha tillgång till effektiva system och förfaranden för att säkerställa att algoritmisk handel inte orsakar eller är ägnad att orsaka otillbörliga handelsförhållanden och att börsen kan hantera alla otillbörliga handelsförhållanden som beror på algoritmisk handel. Börsens system och förfaranden ska omfatta

1) skyldighet för handelsparter att testa sina algoritmer i börsens testmiljö i enlighet med kapitel II och IV i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av dem,

— —

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 5 kap. 1 § i lagen om placeringsfonder

I enlighet med riksdagens beslut
ändras i lagen om placeringsfonder (213/2019) 5 kap. 1 § 1 mom. som följer:

5 kap.

Soliditet och riskhantering

1 §

Fondbolags riskhantering

Ett fondbolag får inte i sin verksamhet ta så stora risker att dess soliditet utsätts för väsentlig fara. Fondbolaget ska ha med hänsyn till verksamheten tillräcklig intern kontroll och tillräckliga riskhanteringssystem. Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.

— —

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av 7 kap. 2 § i lagen om förvaltare av alternativa investeringsfonder

I enlighet med riksdagens beslut
ändras i lagen om förvaltare av alternativa investeringsfonder (162/2014) 7 kap. 2 § 1 mom. som följer:

7 kap.

Organisering av verksamheten

2 §

Rutiner för administration och kontroll

En AIF-förvaltare ska ha tillförlitliga förfaranden för administration och redovisning. Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 1 kap. 13 § och 3 kap. 12 § i lagen om tilläggspensionsstiftelser och tilläggspensionskassor

I enlighet med riksdagens beslut
ändras i lagen om tilläggspensionsstiftelser och tilläggspensionskassor (947/2021) 1 kap. 13 § samt
fogas till 3 kap. 12 § ett nytt 4 mom. som följer:

1 kap.

Tillämpning av lagen och de centrala principerna för verksamheten

13 §

Bestämmelser vars tillämpning beror på antalet försäkrade

På en tilläggspensionsanstalt med färre än 100 försäkrade (*liten tilläggspensionsanstalt*) ska inte 3 kap. 1 och 5–11 §, 12 § 1–3 mom., 13 och 15–17 §, 4 kap. 2 §, 6 kap. 27–35 §, 7 kap. 1 §, 2 § 2 mom., 4, 5 och 8–12 §, 13 kap. och 15 kap. 1–6 och 8–10 § tillämpas.

På en tilläggspensionsanstalt med färre än 16 försäkrade ska, utöver vad som föreskrivs i 1 mom., tillämpas inte 3 kap. 4 § och 12 § 4 mom. och inte heller 6 kap. 3 § och 16 § 1 mom.

3 kap.

Ledningen och företagsstyrningssystemet

12 §

Riktlinjer, system för internkontroll och beredskapsplan

— —

Tilläggspensionsanstaltens nätverks- och informationssystem ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.

———

Denna lag träder i kraft den 20 .

———————

9.

Lag

om ändring av 6 kap. 8 § i försäkringsbolagslagen

I enlighet med riksdagens beslut

ändras i försäkringsbolagslagen (521/2008) 6 kap. 8 § 4 mom., sådant det lyder i lag 981/2013, som följer:

6 kap.

Försäkringsbolagets ledning, företagsstyrningssystem och placering av tillgångar

8 §

Allmänna krav på företagsstyrningen

— —

Försäkringsbolaget ska säkerställa kontinuiteten i verksamheten och att verksamheten bedrivs på ett säkert sätt. I detta syfte ska försäkringsbolaget utarbeta en kontinuitetsplan. Försäkringsbolagets nätverks- och informationssystem ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.

— —

Denna lag träder i kraft den 20 .

10.

Lag

om ändring av 1 § i lagen om aktiebolaget Fonden för industriellt samarbete Ab

I enlighet med riksdagens beslut
fogas till 1 § i lagen om aktiebolaget Fonden för industriellt samarbete Ab (291/1979), sådan paragrafen lyder delvis ändrad i lagarna 1617/1991 och 1083/2000, ett nytt 5 mom. som följer:

1 §

— —

På bolaget tillämpas inte Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

Denna lag träder i kraft den 20 .

11.

Lag

om ändring av 3 § i lagen om statens specialfinansieringsbolag

I enlighet med riksdagens beslut
fogas till 3 § i lagen om statens specialfinansieringsbolag (443/1998), sådan paragrafen lyder delvis ändrad i lag 1545/2011, ett nytt 5 mom. som följer:

3 §

Förvaltning

— —

På bolaget tillämpas inte Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

Denna lag träder i kraft den 20 .

Helsingfors den 6 juni 2024

Statsminister

Petteri Orpo

Näringsminister Wille Rydman

1.

Lag

om ändring av lagen om Finansinspektionen

I enlighet med riksdagens beslut

upphävs i lagen om Finansinspektionen (878/2008) 52 a §, sådan den lyder i lag 959/2018,

ändras 5 § 40 punkten, 38 § 1 mom. 11 punkten, 40 § 2 mom. 11 och 12 punkten, 41 § 3 mom., 50 p § och 71 § 1 mom. 19 punkten,

sådana de lyder, 5 § 40 punkten och 38 § 1 mom. 11 punkten i lag 184/2023, 40 § 2 mom. 11 och 12 punkten i lag 214/2022, 41 § 3 mom. i lag 205/2022, 50 p § i lag 291/2018 och 71 § 1 mom. 19 punkten i lag 524/2021, samt

fogas till 3 § 2 mom., sådant det lyder delvis ändrat i lagarna 1198/2014, 1145/2015, 1442/2016, 445/2023 och 1261/2023, nya 7 och 7 a-punkter i stället för de 7 och 7 a-punkter som upphävts genom lag 1442/2016, till lagen en ny 3 f §, till 5 §, sådan den lyder i lagarna 752/2012, 902/2012, 254/2013, 170/2014, 198/2015, 520/2016, 737/2016, 1442/2016, 228/2017, 575/2017, 893/2017, 1071/2017, 241/2018, 1229/2018, 215/2019, 296/2019, 517/2019, 574/2019, 963/2019, 316/2020, 524/2021, 599/2021, 205/2022, 184/2023 och 192/2023, en ny 41 punkt, till 38 § 1 mom., sådant det lyder i lagarna 752/2012, 254/2013, 1198/2014, 1055/2016, 893/2017, 316/2020, 379/2021, 153/2022, 205/2022 och 184/2023, en ny 12 punkt, till 38 §, sådan den lyder i lagarna 752/2012, 254/2013, 611/2014, 1198/2014, 1055/2016, 893/2017, 316/2020, 379/2021, 153/2022, 205/2022 och 184/2023, ett nytt 7 mom., till 40 § 2 mom., sådant det lyder i lagarna 1071/2017, 1108/2018, 316/2020, 379/2021, 599/2021, 941/2021 och 214/2022, en ny 13 punkt, till 43 §, sådan den lyder i lagarna 176/2016, 1071/2017 och 524/2021, ett nytt 5 mom. och till 71 § 1 mom., sådant det lyder delvis ändrat i lagarna 752/2012, 611/2014, 651/2014, 1198/2014, 505/2015, 520/2016, 1442/2016, 446/2017, 1071/2017, 402/2018, 574/2019, 569/2020, 270/2021 och 524/2021, en ny 20 punkt som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Uppgifter	*Uppgifter*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Finansinspektionen fullgör sina lagstadgade uppgifter genom att	Finansinspektionen fullgör sina lagstadgade uppgifter genom att
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(7–7 a punkten har upphävts genom lag 1442/2016)	7) främja cybersäkra tillvägagångssätt hos finansmarknadsaktörer, 7 a) främja kritiska finansmarknadsaktörers motståndskraft,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Gällande lydelse

Föreslagen lydelse

3 f §

Myndighetssamarbete för att främja cybersäkerhet och motståndskraft

*Finansinspektionen samarbetar med finansministeriet, social- och hälsovårdsministeriet, Finlands Bank, Verket för finansiell stabilitet, Transport- och kommunikationsverket och andra behöriga myndigheter för att hantera störningar relaterade till informations- och kommunikationsteknik (**IKT**) och för att minska konsekvenserna av sådana störningar.*

*Finansinspektionen deltar i myndighetssamarbete enligt artiklarna 32 och 47–49 i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan **EU:s DORA-förordning**, och i verksamheten inom det europeiska ramverket för samordning av åtgärder mot systemiska cyberincidenter samt samarbetar också i övrigt med Europeiska centralbanken, Europeiska systemrisknämnden, Europeiska unionens cybersäkerhetsbyrå, de europeiska tillsynsmyndigheterna, andra EU-myndigheter och utländska EES-tillsynsmyndigheter för att hantera störningar relaterade till informations-och kommunikationsteknik och för att minska konsekvenserna av sådana störningar.*

*Finansinspektionen ska samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (**NIS 2-direktivet**).*

Finansinspektionen ska samarbeta med finansministeriet, inrikesministeriet, Försörjningsberedskapscentralen och andra behöriga myndigheter för skötseln av uppgifter enligt Europaparlamentets och

Gällande lydelse	*Föreslagen lydelse*
	*rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, nedan **CER-direktivet**, för att stärka kritiska aktörers motståndskraft och för att främja frivilligt informationsutbyte mellan dem.*
5 §	5 §
Andra finansmarknadsaktörer	*Andra finansmarknadsaktörer*
Med *andra finansmarknadsaktörer* avses i denna lag	Med *andra finansmarknadsaktörer* avses i denna lag
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
40) den som med stöd av 4 § i lagen om registrering av vissa kreditgivare och kreditförmedlare (186/2023) är skyldig att anmäla sig till det register över kreditgivare och förmedlare av person-till-person-lån som förs av Finansinspektionen.	40) den som med stöd av 4 § i lagen om registrering av vissa kreditgivare och kreditförmedlare (186/2023) är skyldig att anmäla sig till det register över kreditgivare och förmedlare av person-till-person-lån som förs av Finansinspektionen,
	41) sådana tredjepartsleverantörer av IKT-tjänster som avses i artikel 3.19 i EU:s DORA-förordning.
38 §	38 §
Ordningsavgift	*Ordningsavgift*
Finansinspektionen ska ålägga den att betala ordningsavgift som uppsåtligen eller av oaktsamhet	Finansinspektionen ska ålägga den att betala ordningsavgift som uppsåtligen eller av oaktsamhet
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
11) försummar eller bryter mot anmälningsskyldigheten enligt 8 § 3 mom. i lagen om registrering av vissa kreditgivare och kreditförmedlare.	11) försummar eller bryter mot anmälningsskyldigheten enligt 8 § 3 mom. i lagen om registrering av vissa kreditgivare och kreditförmedlare,
	12) försummar eller bryter mot skyldigheten att hantera IKT-risker enligt artikel 16 i EU:s DORA-förordning.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Om ordningsavgift påförs med stöd av 1 mom. 12 punkten, ska artikel 51.2 i EU:s DORA-förordning iakttas i stället för 2 mom. i fråga om de omständigheter som ska beaktas vid bedömningen av ordningsavgiftens belopp.

Gällande lydelse	*Föreslagen lydelse*
40 §	40 §
Påföljdsavgift	*Påföljdsavgift*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Påföljdsavgift ska också påföras den som uppsåtligen eller av oaktsamhet försummar eller bryter mot	Påföljdsavgift ska också påföras den som uppsåtligen eller av oaktsamhet försummar eller bryter mot
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
11) bestämmelserna i artikel 5 i Europaparlamentets och rådets förordning (EU) 2020/852 om inrättande av en ram för att underlätta hållbara investeringar och om ändring av förordning (EU) 2019/2088, nedan *taxonomiförordningen*, om transparens i fråga om miljömässigt hållbara investeringar i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, bestämmelserna i artikel 6 om transparens i fråga om finansiella produkter som främjar miljörelaterade egenskaper i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, eller bestämmelserna i artikel 7 om transparens i fråga om andra finansiella produkter i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, *eller*	11) bestämmelserna i artikel 5 i Europaparlamentets och rådets förordning (EU) 2020/852 om inrättande av en ram för att underlätta hållbara investeringar och om ändring av förordning (EU) 2019/2088, nedan *taxonomiförordningen*, om transparens i fråga om miljömässigt hållbara investeringar i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, bestämmelserna i artikel 6 om transparens i fråga om finansiella produkter som främjar miljörelaterade egenskaper i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter, eller bestämmelserna i artikel 7 om transparens i fråga om andra finansiella produkter i upplysningar som lämnas innan avtal ingås och i regelbundna rapporter,
12) bestämmelserna i artiklarna 5–7 i PEPP-förordningen om registreringsskyldighet och bestämmelserna om lämnande av falska eller vilseledande uppgifter som grund för registreringen av en PEPP-produkt i det centrala offentliga register som förs av Europeiska försäkrings- och tjänstepensionsmyndigheten, bestämmelserna i artikel 18 om erbjudande av portabilitetsmöjlighet, bestämmelserna i artikel 19 om användning av underkonton för PEPP-produkter, bestämmelserna i artikel 20 om skyldighet att lämna information i anknytning till öppnande av ett nytt underkonto, bestämmelserna i artikel 21 om information om portabilitet till de behöriga myndigheterna, bestämmelserna i artikel 22 om en allmän princip som gäller PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 23 om distributionsregler för olika typer av PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 24 om elektronisk	12) bestämmelserna i artiklarna 5–7 i PEPP-förordningen om registreringsskyldighet och bestämmelserna om lämnande av falska eller vilseledande uppgifter som grund för registreringen av en PEPP-produkt i det centrala offentliga register som förs av Europeiska försäkrings- och tjänstepensionsmyndigheten, bestämmelserna i artikel 18 om erbjudande av portabilitetsmöjlighet, bestämmelserna i artikel 19 om användning av underkonton för PEPP-produkter, bestämmelserna i artikel 20 om skyldighet att lämna information i anknytning till öppnande av ett nytt underkonto, bestämmelserna i artikel 21 om information om portabilitet till de behöriga myndigheterna, bestämmelserna i artikel 22 om en allmän princip som gäller PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 23 om distributionsregler för olika typer av PEPP-sparinstitut och PEPP-distributörer, bestämmelserna i artikel 24 om elektronisk

Gällande lydelse	*Föreslagen lydelse*
distribution och om användning av andra varaktiga medier, bestämmelserna i artikel 25 om krav på produkt-övervakning och produktstyrning, bestämmelserna i artikel 26 om PEPP-faktablad, bestämmelserna i artikel 27 om PEPP-faktabladets språk, bestämmelserna i artikel 28 om PEPP-faktabladets innehåll, bestämmelserna i artikel 29 om marknadsföringsmaterial, bestämmelserna i artikel 30 om översyn av PEPP-faktabladet, bestämmelserna i artikel 31 om skadeståndsansvar, bestämmelserna i artikel 32 om PEPP-avtal som täcker biometriska risker, bestämmelserna i artikel 33 om tillhandahållande av PEPP-faktabladet, bestämmelserna i artikel 34 om specifikation av PEPP-kundens krav och behov samt tillhandahållande av rådgivning, bestämmelserna i artikel 35 om allmänna bestämmelser som gäller PEPP-pensionsbesked, bestämmelserna i artikel 36 om innehållet i PEPP-pensionsbeskedet, bestämmelserna i artikel 37 om kompletterande information i PEPP-pensionsbeskedet, bestämmelserna i artikel 38 om information som ska lämnas till PEPP-sparare under tiden före pensionering och till PEPP-förmånstagare under utbetalningsfasen, bestämmelserna i artikel 39 om information som på begäran ska lämnas till PEPP-sparare och PEPP-förmånstagare, bestämmelserna i artikel 40 om allmänna bestämmelser som gäller rapportering till nationella myndigheter, bestämmelserna i artikel 41 om investeringsregler under intjänandefasen, bestämmelserna i artikel 42 om allmänna bestämmelser som gäller PEPP-spararens investeringsalternativ, bestämmelserna i artikel 43 om PEPP-spararens val av investeringsalternativ, bestämmelserna i artikel 44 om villkor för ändring av det valda investeringsalternativet, bestämmelserna i artikel 45 om bas-PEPP-produkten, bestämmelserna i artikel 46 om riskreduceringstekniker, bestämmelserna i artikel 47 om villkor som rör intjänandefasen, bestämmelserna i artikel 48 om förvaringsinstitutets förvarings- och övervakningsuppgifter, bestämmelserna i artikel 50 om hantering av klagomål från	distribution och om användning av andra varaktiga medier, bestämmelserna i artikel 25 om krav på produkt-övervakning och produktstyrning, bestämmelserna i artikel 26 om PEPP-faktablad, bestämmelserna i artikel 27 om PEPP-faktabladets språk, bestämmelserna i artikel 28 om PEPP-faktabladets innehåll, bestämmelserna i artikel 29 om marknadsföringsmaterial, bestämmelserna i artikel 30 om översyn av PEPP-faktabladet, bestämmelserna i artikel 31 om skadeståndsansvar, bestämmelserna i artikel 32 om PEPP-avtal som täcker biometriska risker, bestämmelserna i artikel 33 om tillhandahållande av PEPP-faktabladet, bestämmelserna i artikel 34 om specifikation av PEPP-kundens krav och behov samt tillhandahållande av rådgivning, bestämmelserna i artikel 35 om allmänna bestämmelser som gäller PEPP-pensionsbesked, bestämmelserna i artikel 36 om innehållet i PEPP-pensionsbeskedet, bestämmelserna i artikel 37 om kompletterande information i PEPP-pensionsbeskedet, bestämmelserna i artikel 38 om information som ska lämnas till PEPP-sparare under tiden före pensionering och till PEPP-förmånstagare under utbetalningsfasen, bestämmelserna i artikel 39 om information som på begäran ska lämnas till PEPP-sparare och PEPP-förmånstagare, bestämmelserna i artikel 40 om allmänna bestämmelser som gäller rapportering till nationella myndigheter, bestämmelserna i artikel 41 om investeringsregler under intjänandefasen, bestämmelserna i artikel 42 om allmänna bestämmelser som gäller PEPP-spararens investeringsalternativ, bestämmelserna i artikel 43 om PEPP-spararens val av investeringsalternativ, bestämmelserna i artikel 44 om villkor för ändring av det valda investeringsalternativet, bestämmelserna i artikel 45 om bas-PEPP-produkten, bestämmelserna i artikel 46 om riskreduceringstekniker, bestämmelserna i artikel 47 om villkor som rör intjänandefasen, bestämmelserna i artikel 48 om förvaringsinstitutets förvarings- och övervakningsuppgifter, bestämmelserna i artikel 50 om hantering av klagomål från

Gällande lydelse	*Föreslagen lydelse*
PEPP-kunder, bestämmelserna i artikel 52 om tillhandahållande av bytesmöjlighet, bestämmelserna i artikel 53 om inledande av byte, bestämmelserna i artikel 54 om avgifter och kostnader i samband med byte, bestämmelserna i artikel 55 om skydd av PEPP-sparare mot finansiell förlust eller bestämmelserna i artikel 56 om information om bytesmöjligheten.	PEPP-kunder, bestämmelserna i artikel 52 om tillhandahållande av bytesmöjlighet, bestämmelserna i artikel 53 om inledande av byte, bestämmelserna i artikel 54 om avgifter och kostnader i samband med byte, bestämmelserna i artikel 55 om skydd av PEPP-sparare mot finansiell förlust eller bestämmelserna i artikel 56 om information om bytesmöjligheten*,* *13) bestämmelserna om hantering av IKT-risker i artiklarna 5–14 i EU:s DORA-förordning, bestämmelserna om hantering av, klassificering av och rapportering om IKT-relaterade incidenter i artiklarna 17–19 i den förordningen, bestämmelserna om testning av digital operativ motståndskraft i artiklarna 24–27 i den förordningen eller bestämmelserna om hantering av IKT-tredjepartsrisker i artiklarna 28–30 i den förordningen, vilka är förpliktande för i artikel 2.2 i den förordningen avsedda finansiella entiteter*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
41 §	41 §
Påförande av påföljdsavgift	*Påförande av påföljdsavgift*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Om det är fråga om överträdelse av förordningen om referensvärden, ska utöver det som föreskrivs i 2 mom. också förfarandets inverkan på realekonomin beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av Europaparlamentets och rådets förordning (EU) 2017/1129 om prospekt som ska offentliggöras när värdepapper erbjuds till allmänheten eller tas upp till handel på en reglerad marknad, och om upphävande av direktiv 2003/71/EG, nedan *prospektförordningen*, ska överträdelsens inverkan också på icke-professionella kunders ställning beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av EU:s gräsrotsfinansieringsförordning ska överträdelsens inverkan på investerarnas	Om det är fråga om överträdelse av förordningen om referensvärden, ska utöver det som föreskrivs i 2 mom. också förfarandets inverkan på realekonomin beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av Europaparlamentets och rådets förordning (EU) 2017/1129 om prospekt som ska offentliggöras när värdepapper erbjuds till allmänheten eller tas upp till handel på en reglerad marknad, och om upphävande av direktiv 2003/71/EG, nedan *prospektförordningen*, ska överträdelsens inverkan också på icke-professionella kunders ställning beaktas vid bedömningen av påföljdsavgiftens belopp. Om det är fråga om överträdelse av EU:s gräsrotsfinansieringsförordning ska överträdelsens inverkan på investerarnas intressen beaktas vid bedömningen av

Gällande lydelse	*Föreslagen lydelse*
intressen beaktas vid bedömningen av påföljdsavgiftens belopp.	påföljdsavgiftens belopp. *Om det är fråga om överträdelse av EU:s DORA-förordning, ska artikel 51.2 i den förordningen iakttas i stället för 2 mom. vid bedömningen av påföljdsavgiftens belopp.*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
43 §	43 §
Offentliggörande av administrativa påföljder och andra beslut	*Offentliggörande av administrativa påföljder och andra beslut*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
	Om ordningsavgift, offentlig varning eller påföljdsavgift påförs på grund av en överträdelse av EU:s DORA-förordning, ska artikel 54 i EU:s DORA-förordning tillämpas i stället för denna paragraf på offentliggörandet av beslutet.
50 p §	50 p §
Behörig myndighet enligt direktivet om nät- och informationssäkerhet	*Behörig myndighet enligt **EU:s DORA-förordning, NIS 2-direktivet och CER-direktivet***
Finansinspektionen är behörig myndighet enligt artikel 8.1 i Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, nedan *direktivet om nät- och informationssäkerhet*, när det gäller sektorerna 3 och 4 i bilaga II till direktivet.	*Finansinspektionen är den behöriga myndighet som avses i artikel 46 i EU:s DORA-förordning och den myndighet som avses i artikel 26.9 i den förordningen.* *Finansinspektionen är den behöriga myndighet som avses i artikel 8.1 i NIS 2-direktivet i fråga om sektorerna 3 och 4 i bilaga I till direktivet.* *Finansinspektionen är den behöriga myndighet som avses i artikel 9.1 i CER-direktivet i fråga om sektorerna 3 och 4 i bilagan till direktivet.*
52 a §	(upphävs)
Samarbete och utbyte av information vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet	
Finansinspektionen ska samarbeta med Transport- och kommunikationsverket vid skötseln av uppgifter enligt direktivet om nät-	

Gällande lydelse	*Föreslagen lydelse*
och informationssäkerhet. Finansinspektionen har för detta syfte rätt att trots bestämmelserna om sekretess lämna ut uppgifter till Transport- och kommunikationsverket.	
71 §	71 §
Rätt och skyldighet att lämna ut information	*Rätt och skyldighet att lämna ut information*
Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Finansinspektionen utan hinder av sekretessbestämmelserna rätt att lämna ut information till	Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Finansinspektionen utan hinder av sekretessbestämmelserna rätt att lämna ut information till
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
19) Europeiska kommissionen när sådan information i anknytning till tillsynen över finansmarknaden krävs för att kommissionen ska kunna utöva sina befogenheter.	19) Europeiska kommissionen när sådan information i anknytning till tillsynen över finansmarknaden krävs för att kommissionen ska kunna utöva sina befogenheter,
	20) Transport- och kommunikationsverket för genomförande av det samarbete som avses i 3 f § 3 mom., när det gäller störningar och hot relaterade till informations- och kommunikationsteknik.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 9 och 11 kap. i kreditinstitutslagen

I enlighet med riksdagens beslut

ändras i kreditinstitutslagen (610/2014) 9 kap. 2 § 1 mom. och 16 § 3 mom. samt 11 kap. 2 § 2 mom. 10 punkten,

av dem 11 kap. 2 § 2 mom. 10 punkten sådan den lyder i lag 233/2021, samt

fogas till 11 kap. 2 § 2 mom., sådant det lyder i lag 233/2021, en ny 11 punkt som följer:

Gällande lydelse	*Föreslagen lydelse*
9 kap.	9 kap.
Riskhantering	**Riskhantering**
2 §	2 §
Allmänna krav som ska ställas på riskhanteringssystem	*Allmänna krav som ska ställas på riskhanteringssystem*
Ett kreditinstitut ska ha effektiva, tillförlitliga och dokumenterade förvaltnings- och styrningssystem för identifiering, hantering, begränsning, övervakning och rapportering av nuvarande och framtida risker som kreditinstitutet och dess verksamhet exponeras för. Systemen ska omfatta	Ett kreditinstitut ska ha effektiva, tillförlitliga och dokumenterade förvaltnings- och styrningssystem för identifiering, hantering, begränsning, övervakning och rapportering av nuvarande och framtida risker som kreditinstitutet och dess verksamhet exponeras för. Systemen ska omfatta
1) en tydlig organisationsstruktur med väldefinierade och konsekventa befogenhets- och ansvarsförhållanden,	1) en tydlig organisationsstruktur med väldefinierade och konsekventa befogenhets- och ansvarsförhållanden,
2) effektiva rapporteringsprocesser för riskhanteringen,	2) effektiva rapporteringsprocesser för riskhanteringen,
3) sunda processer för intern kontroll, inklusive förvaltnings- och redovisningsrutiner,	3) sunda processer för intern kontroll, inklusive förvaltnings- och redovisningsrutiner,
	4) nätverks- och informationssystem enligt Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan ***EU:s DORA-förordning****, och de bestämmelser som utfärdats med stöd av den,*
4) en ersättningspolicy och -praxis som är förenlig med och främjar sund och effektiv riskhantering.	*5*) en ersättningspolicy och *ersättnings*praxis som är förenlig med och främjar sund och effektiv riskhantering.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
16 §	16 §
Operativ risk	*Operativ risk*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Kreditinstitutet ska ha beredskaps- och kontinuitetsplaner för att bereda sig för allvarliga störningar i affärsverksamheten samt säkerställa sin förmåga att fortlöpande bedriva verksamhet och begränsa förlusterna i störningssituationer.	Kreditinstitutet ska ha beredskaps- och kontinuitetsplaner för att bereda sig för allvarliga störningar i affärsverksamheten samt säkerställa sin förmåga att fortlöpande bedriva verksamhet och begränsa förlusterna i störningssituationer. *Bestämmelser om den*

Gällande lydelse	*Föreslagen lydelse*
	*kontinuitetspolicy och de kontinuitetsplaner för informations- och kommunikationstekniken (**IKT**) i kreditinstitutets affärsverksamhet och de åtgärds- och återställningsplaner avseende IKT som ska ingå i de nämnda planerna finns i artikel 11 i EU:s DORA-förordning.*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
11 kap.	11 kap.
Tillsyn över kreditinstitut	**Tillsyn över kreditinstitut**
2 §	2 §
Tillsynsmyndighetens bedömning	*Tillsynsmyndighetens bedömning*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
Tillsynsmyndigheten ska i sin bedömning enligt 1 mom. beakta åtminstone	Tillsynsmyndigheten ska i sin bedömning enligt 1 mom. beakta åtminstone
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
10) den ränterisk i den finansiella balansräkningen som riktar sig mot kreditinstitutet.	10) den ränterisk i den finansiella balansräkningen som riktar sig mot kreditinstitutet,
	11) de risker som framkommer vid testningen av den digitala operativa motståndskraften enligt kapitel IV i EU:s DORA-förordning.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 7 kap. 2 § och 7 a kap. 1 § i lagen om investeringstjänster

I enlighet med riksdagens beslut

ändras i lagen om investeringstjänster (747/2012) 7 kap. 2 § 3–5 mom. och 7 a kap. 1 § 1 mom. 1 punkten och 2 mom., sådana de lyder i lag 1069/2017, som följer:

Gällande lydelse	*Föreslagen lydelse*
7 kap.	7 kap.
Organisering av värdepappersföretags verksamhet	**Organisering av värdepappersföretags verksamhet**
2 §	2 §
Tillförlitlig organisering av verksamheten	*Tillförlitlig organisering av verksamheten*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Värdepappersföretaget ska vidta rimliga åtgärder för att säkerställa kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och bedrivandet av investeringsverksamhet.	Värdepappersföretaget ska vidta rimliga åtgärder för att säkerställa kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och bedrivandet av investeringsverksamhet.
Värdepappersföretaget ska i det syftet använda ändamålsenliga och proportionella system, resurser och förfaranden.	Värdepappersföretaget ska i det syftet använda ändamålsenliga och proportionella system, resurser och förfaranden. *Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan* ***EU:s DORA-förordning****, och de bestämmelser som utfärdats med stöd av den.*
Värdepappersföretaget ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för intern kontroll, effektiva riskbedömningsmetoder *samt effektiva kontroll- och skyddssystem för sina informationsbehandlingssystem*.	Värdepappersföretaget ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för intern kontroll och effektiva riskbedömningsmetoder.
Värdepappersföretaget ska, utan att begränsa Finansinspektionens tillgång till information, ha inrättat sunda skyddsmekanismer för att garantera skyddet och autentiseringen vid informationsöverföringen, minimera risken för dataförvanskning och för obehörig åtkomst samt förhindra informationsläckor så att uppgifterna alltid behandlas konfidentiellt.	Värdepappersföretaget ska, utan att begränsa Finansinspektionens tillgång till information, ha inrättat sunda skyddsmekanismer för att garantera skyddet och autentiseringen vid informationsöverföringen *i enlighet med EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av den*, minimera risken för dataförvanskning och för obehörig åtkomst samt förhindra informationsläckor så att uppgifterna alltid behandlas konfidentiellt.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
7 a kap.	7 a kap.
Algoritmisk handel och direkt elektroniskt tillträde till en handelsplats	**Algoritmisk handel och direkt elektroniskt tillträde till en handelsplats**
1 §	1 §
Algoritmisk handel	*Algoritmisk handel*
Ett värdepappersföretag som bedriver algoritmisk handel ska ha inrättat effektiva system och riskkontroller som är anpassade för den verksamhet som drivs för att 1) säkerställa att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet samt att de omfattas av lämpliga handelströsklar och handelslimiter,	Ett värdepappersföretag som bedriver algoritmisk handel ska ha inrättat effektiva system och riskkontroller som är anpassade för den verksamhet som drivs för att 1) säkerställa att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet *i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det* samt att de omfattas av lämpliga handelströsklar och handelslimiter,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Ett värdepappersföretag som avses i 1 mom. ska ha inrättat effektiva arrangemang för driftskontinuitet för att hantera avbrott av driften i sina handelssystem. Värdepappersföretaget ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller kraven som föreskrivs i 1 och 2 mom.	Ett värdepappersföretag som avses i 1 mom. ska *dessutom* ha inrättat effektiva arrangemang för driftskontinuitet för att hantera avbrott av driften i sina handelssystem. *Värdepappersföretaget ska ha en sådan kontinuitetspolicy och sådana kontinuitetsplaner för informations- och kommunikationsteknik (**IKT**) samt sådana åtgärds- och återställningsplaner avseende IKT som avses i artikel 11 i EU:s DORA-förordning.* Värdepappersföretaget ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller *de krav* som föreskrivs i 1 och 2 mom. *och i EU:s DORA-förordning och med stöd av den*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 19 a och 19 b § i lagen om betalningsinstitut

I enlighet med riksdagens beslut

ändras i lagen om betalningsinstitut (297/2010) 19 a § 1 mom. och 19 b §, sådana de lyder i lag 890/2017, som följer:

Gällande lydelse	*Föreslagen lydelse*
19 a §	19 a §
Hantering av operativa risker och säkerhetsrisker	*Hantering av operativa risker och säkerhetsrisker*
Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska inrätta ett tillräckligt riskhanteringssystem med riskhanteringsåtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker i anslutning till de betaltjänster som de tillhandahåller. De ska ha ett effektivt incidenthanteringsförfarande och kunna upptäcka och klassificera allvarliga operativa incidenter och säkerhetsincidenter.	Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska inrätta ett tillräckligt riskhanteringssystem med riskhanteringsåtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker i anslutning till de betaltjänster som de tillhandahåller. De ska ha ett effektivt incidenthanteringsförfarande och kunna upptäcka och klassificera allvarliga operativa incidenter och säkerhetsincidenter. *Bestämmelserna i detta moment begränsar inte tillämpningen av kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan* ***EU:s DORA-förordning****, och de bestämmelser som utfärdats med stöd av det.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
19 b §	19 b §
Anmälan om incidenter och bedrägerier	*Anmälan om incidenter och bedrägerier*
Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska utan obefogat dröjsmål anmäla allvarliga operativa incidenter och säkerhetsincidenter som de upptäcker till Finansinspektionen. Om en incident har påverkat eller kan ha påverkat betaltjänstanvändarnas ekonomiska	

Gällande lydelse	*Föreslagen lydelse*
intressen, ska också betaltjänstanvändarna informeras om incidenten. Betaltjänstanvändarna ska samtidigt informeras om de sätt på vilka de kan minska incidentens negativa effekter. Finansinspektionen får meddela närmare föreskrifter om klassificeringen av operativa incidenter och säkerhetsincidenter som avses i detta moment och om innehållet, formatet och förfarandet i fråga om en anmälan.	
Ett kontoförande betalningsinstitut och en person som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § ska göra en anmälan till Finansinspektionen, om de upptäcker att en leverantör av kontoinformationstjänster eller en leverantör av betalningsinitieringstjänster använder ett betalkonto på ett obehörigt eller bedrägligt sätt och det kontoförande betalningsinstitutet eller den som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § på denna grund förhindrar leverantörens tillträde till betalkontot. Anmälan ska innehålla tillräcklig information om incidenten och om åtgärder med anledning av den. Finansinspektionen ska bedöma fallet och vidta behövliga åtgärder.	Ett kontoförande betalningsinstitut och en person som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § ska göra en anmälan till Finansinspektionen, om de upptäcker att en leverantör av kontoinformationstjänster eller en leverantör av betalningsinitieringstjänster använder ett betalkonto på ett obehörigt eller bedrägligt sätt och det kontoförande betalningsinstitutet eller den som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § på denna grund förhindrar leverantörens tillträde till betalkontot. Anmälan ska innehålla tillräcklig information om incidenten och om åtgärder med anledning av den. Finansinspektionen ska bedöma fallet och vidta behövliga åtgärder.
Efter att ha fått en i 1 mom. avsedd anmälan ska Finansinspektionen utan obefogat dröjsmål informera Europeiska bankmyndigheten och Europeiska centralbanken om incidenten. Finansinspektionen ska i samarbete med Europeiska bankmyndigheten och Europeiska centralbanken bedöma incidentens relevans för de nationella myndigheterna i staterna inom Europeiska ekonomiska samarbetsområdet och i andra länder. Finansinspektionen ska vid behov också informera andra berörda finländska myndigheter om incidenten.	
Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska minst en gång per år lämna Finansinspektionen statistiska uppgifter om bedrägerier i samband med betalningsinstrument. Finansinspektionen ska lämna Europeiska bankmyndigheten och	Betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 § och sådana leverantörer av kontoinformationstjänster som avses i 7 b § ska minst en gång per år lämna Finansinspektionen statistiska uppgifter om bedrägerier i samband med betalningsinstrument. Finansinspektionen ska lämna Europeiska bankmyndigheten och Europeiska centralbanken dessa uppgifter i aggregerad form. Finansinspektionen får meddela närmare föreskrifter om den

Gällande lydelse	*Föreslagen lydelse*
Europeiska centralbanken dessa uppgifter i aggregerad form. Finansinspektionen får meddela närmare föreskrifter om den rapporteringsskyldighet som avses i detta moment. Vad som föreskrivs *ovan* i denna paragraf tillämpas inte på institut för elektroniska pengar.	rapporteringsskyldighet som avses i detta moment. Vad som föreskrivs i *1 och 2 mom.* tillämpas inte på institut för elektroniska pengar. *Bestämmelser om skyldigheten för betalningsinstitut, personer som tillhandahåller betaltjänster med stöd av ett undantag enligt 7 §, sådana leverantörer av kontoinformationstjänster som avses i 7 b § och utgivare av elektroniska pengar att anmäla incidenter relaterade till informations- och kommunikationsteknik samt betalningsrelaterade operativa incidenter eller säkerhetsincidenter finns i kapitel III i EU:s DORA-förordning.*
	Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 3 kap. 1 och 18 § i lagen om handel med finansiella instrument

I enlighet med riksdagens beslut
ändras i lagen om handel med finansiella instrument (1070/2017) 3 kap. 1 § 1, 3 och 5 mom. samt 18 § 1 mom. 1 punkten, sådana de lyder i lag 295/2019, som följer:

Gällande lydelse	*Föreslagen lydelse*
3 kap.	3 kap.
Organisering av verksamheten på en reglerad marknad	**Organisering av verksamheten på en reglerad marknad**
1 §	1 §
Krav som gäller organisering av verksamheten på en reglerad marknad	*Krav som gäller organisering av verksamheten på en reglerad marknad*
En börs ska organisera sin verksamhet på ett tillförlitligt sätt med beaktande av arten och omfattningen av dess affärsverksamhet. Börsen ska i alla situationer säkerställa den	En börs ska organisera sin verksamhet på ett tillförlitligt sätt med beaktande av arten och omfattningen av dess affärsverksamhet. Börsen ska i alla situationer säkerställa den verksamhetsrelaterade riskhanteringen och

Gällande lydelse	*Föreslagen lydelse*
verksamhetsrelaterade riskhanteringen och verksamhetens kontinuitet.	verksamhetens kontinuitet. *Börsen ska hantera risker relaterade till informations- och kommunikationsteknik (**IKT**) i enlighet med kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, nedan **EU:s DORA-förordning**, och de bestämmelser som utfärdats med stöd av det.*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
Börsen ska säkerställa *att dess system och förfaranden också i störningssituationer tryggar* tillförlitligheten och kontinuiteten i handelssystemet. Börsen *ska säkerställa att dess* handelssystem är motståndskraftiga, har tillräcklig kapacitet för att hantera toppbelastning i fråga om order- och meddelandevolymer och *säkerställa* ordnad handel under svåra förhållanden på marknaden. Börsen ska regelbundet testa handelssystemets funktion med belastningstestför att uppfylla de krav som beskrivs ovan.	Börsen ska säkerställa tillförlitligheten och kontinuiteten i handelssystemet *också i störningssituationer*. Börsen *ska ha operativ motståndskraft, som den ska upprätthålla i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det, så att börsens* handelssystem är *tillräckligt* motståndskraftiga, *att den* har tillräcklig kapacitet för att hantera toppbelastning i fråga om order- och meddelandevolymer och *att den kan upprätthålla* ordnad handel under svåra förhållanden på marknaden. *För att säkerställa kontinuiteten i tjänsterna på en reglerad marknad ska börsen ha en sådan IKT-kontinuitetspolicy och sådana IKT-kontinuitetsplaner samt sådana åtgärds- och återställningsplaner avseende IKT som avses i artikel 11 i EU:s DORA-förordning.* Börsen ska regelbundet testa handelssystemets funktion med belastningstest för att uppfylla de krav som nämns ovan.
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
Vad som i 1 mom. föreskrivs om börser ska på motsvarande sätt tillämpas på börsers holdingföretag.	Vad som i 1 mom. föreskrivs om börser ska på motsvarande sätt tillämpas på börsers holdingföretag*, med undantag för skyldigheten att hantera IKT-relaterade risker i enlighet med kapitel II i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av det*.
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
18 §	18 §
Algoritmisk handel	*Algoritmisk handel*

Gällande lydelse	*Föreslagen lydelse*
En börs ska ha tillgång till effektiva system och förfaranden för att säkerställa att algoritmisk handel inte orsakar eller är ägnad att orsaka otillbörliga handelsförhållanden och att börsen kan hantera alla otillbörliga handelsförhållanden som beror på algoritmisk handel. Börsens system och förfaranden ska omfatta	En börs ska ha tillgång till effektiva system och förfaranden för att säkerställa att algoritmisk handel inte orsakar eller är ägnad att orsaka otillbörliga handelsförhållanden och att börsen kan hantera alla otillbörliga handelsförhållanden som beror på algoritmisk handel. Börsens system och förfaranden ska omfatta
1) skyldighet för handelsparter att testa sina algoritmer i börsens testmiljö,	1) skyldighet för handelsparter att testa sina algoritmer i börsens *testmiljö i enlighet med kapitel II och IV i EU:s DORA-förordning och de bestämmelser som utfärdats med stöd av dem*,
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 5 kap. 1 § i lagen om placeringsfonder

I enlighet med riksdagens beslut
ändras i lagen om placeringsfonder (213/2019) 5 kap. 1 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
5 kap.	5 kap.
Soliditet och riskhantering	**Soliditet och riskhantering**
1 §	1 §
Fondbolags riskhantering	*Fondbolags riskhantering*
Ett fondbolag får inte i sin verksamhet ta så stora risker att dess soliditet utsätts för väsentlig fara. Fondbolaget ska ha med hänsyn till verksamheten tillräcklig intern kontroll och tillräckliga riskhanteringssystem.	Ett fondbolag får inte i sin verksamhet ta så stora risker att dess soliditet utsätts för väsentlig fara. Fondbolaget ska ha med hänsyn till verksamheten tillräcklig intern kontroll och tillräckliga riskhanteringssystem. *Kontroll- och säkerhetsarrangemangen för elektronisk databehandling ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital*

Gällande lydelse	*Föreslagen lydelse*
— — — — — — — — — — — — — — —	*operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.* — — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

7.

Lag

om ändring av 7 kap. 2 § i lagen om förvaltare av alternativa investeringsfonder

I enlighet med riksdagens beslut
ändras i lagen om förvaltare av alternativa investeringsfonder (162/2014) 7 kap. 2 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
7 kap.	7 kap.
Organisering av verksamheten	**Organisering av verksamheten**
2 §	2 §
Rutiner för administration och kontroll	*Rutiner för administration och kontroll*
En AIF-förvaltare ska ha tillförlitliga förfaranden för administration och redovisning *och tillförlitliga* kontroll- och säkerhetsrutiner för elektronisk databehandling.	En AIF-förvaltare ska ha tillförlitliga förfaranden för administration och redovisning. *K*ontroll- och säkerhets*arrangemangen* för elektronisk databehandling *ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 1 kap. 13 § och 3 kap. 12 § i lagen om tilläggspensionsstiftelser och tilläggspensionskassor

I enlighet med riksdagens beslut

ändras i lagen om tilläggspensionsstiftelser och tilläggspensionskassor (947/2021) 1 kap. 13 § samt

fogas till 3 kap. 12 § ett nytt 4 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
1 kap.	1 kap.
Tillämpning av lagen och de centrala principerna för verksamheten	**Tillämpning av lagen och de centrala principerna för verksamheten**
13 §	13 §
Bestämmelser vars tillämpning beror på antalet försäkrade	*Bestämmelser vars tillämpning beror på antalet försäkrade*
På en tilläggspensionsanstalt med färre än 100 försäkrade (liten tilläggspensionsanstalt) ska inte 3 kap. 1, 5–13 och 15–17 §, 4 kap. 2 §, 6 kap. 27–35 §, 7 kap. 1 §, 2 § 2 mom., 4, 5 och 8–12 §, 13 kap. och 15 kap. 1–6 och 8–10 § tillämpas.	På en tilläggspensionsanstalt med färre än 100 försäkrade (*liten tilläggspensionsanstalt*) ska inte 3 kap. 1 och 5–*11 §, 12 § 1–3 mom.,* 13 och 15–17 §, 4 kap. 2 §, 6 kap. 27–35 §, 7 kap. 1 §, 2 § 2 mom., 4, 5 och 8–12 §, 13 kap. och 15 kap. 1–6 och 8–10 § tillämpas.
På en tilläggspensionsanstalt med färre än 16 försäkrade ska inte 3 kap. 4 § eller 6 kap. 3 § och 16 § 1 mom. *tillämpas*.	På en tilläggspensionsanstalt med färre än 16 försäkrade ska*, utöver vad som föreskrivs i 1 mom., tillämpas* inte 3 kap. 4 § *och 12 § 4 mom. och inte heller* 6 kap. 3 § och 16 § 1 mom.
3 kap.	3 kap.
Ledningen och företagsstyrningssystemet	**Ledningen och företagsstyrningssystemet**
12 §	12 §
Riktlinjer, system för internkontroll och beredskapsplan	*Riktlinjer, system för internkontroll och beredskapsplan*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
	Tilläggspensionsanstaltens nätverks- och informationssystem ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.
	————
	Denna lag träder i kraft den 20 .

9.

Lag

om ändring av 6 kap. 8 § i försäkringsbolagslagen

I enlighet med riksdagens beslut
ändras i försäkringsbolagslagen (521/2008) 6 kap. 8 § 4 mom., sådant det lyder i lag 981/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
6 kap.	6 kap.
Försäkringsbolagets ledning, företagsstyrningssystem och placering av tillgångar	**Försäkringsbolagets ledning, företagsstyrningssystem och placering av tillgångar**
8 §	8 §
Allmänna krav på företagsstyrningen	*Allmänna krav på företagsstyrningen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Försäkringsbolaget ska säkerställa kontinuiteten i verksamheten och att verksamheten bedrivs på ett säkert sätt. I detta syfte ska försäkringsbolaget utarbeta en kontinuitetsplan.	Försäkringsbolaget ska säkerställa kontinuiteten i verksamheten och att verksamheten bedrivs på ett säkert sätt. I detta syfte ska försäkringsbolaget utarbeta en kontinuitetsplan. *Försäkringsbolagets nätverks- och informationssystem ska överensstämma med Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och*

Gällande lydelse	*Föreslagen lydelse*
	om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 och de bestämmelser som utfärdats med stöd av den.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

10.

Lag

om ändring av 1 § i lagen om aktiebolaget Fonden för industriellt samarbete Ab

I enlighet med riksdagens beslut

fogas till 1 § i lagen om aktiebolaget Fonden för industriellt samarbete Ab (291/1979), sådan paragrafen lyder delvis ändrad i lagarna 1617/1991 och 1083/2000, ett nytt 5 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	På bolaget tillämpas inte Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.
	Denna lag träder i kraft den 20 .

11.

Lag

om ändring av 3 § i lagen om statens specialfinansieringsbolag

I enlighet med riksdagens beslut

fogas till 3 § i lagen om statens specialfinansieringsbolag (443/1998), sådan paragrafen lyder delvis ändrad i lag 1545/2011, ett nytt 5 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Förvaltning	*Förvaltning*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	På bolaget tillämpas inte Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.
	Denna lag träder i kraft den 20 .