Beslutspromemoria

Datum 2024-12-18 FI dnr 24-1341

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Nya och ändrade föreskrifter och allmänna råd till följd av Dora-förordningen

Sammanfattning

EU:s förordning om digital operativ motståndskraft för finanssektorn[1] (Dora-förordningen) ska börja tillämpas den 17 januari 2025. I förordningen finns enhetliga regler för riskhantering som avser informations- och kommunikationsteknologi (IKT), rapportering av IKT-relaterade incidenter, testning av företags digitala beredskap, riskhantering av tredjepartsleverantörer av IKT-tjänster samt informationsdelning.

Finansinspektionen (FI) beslutar om ändringar i FI:s föreskrifter och allmänna råd för att anpassa dem till det nya regelverket. Eftersom Dora-förordningen gäller för de flesta typer av företag inom finanssektorn görs ändringar i olika föreskrifter som gäller för olika delar av finanssektorn.

FI beslutar även om nya föreskrifter där det anges vilket tekniskt format som företagen ska använda vid rapportering till FI enligt Dora-förordningen samt vid vilken tidpunkt som de ska rapportera in informationsregister enligt Dora-förordningen.

De nya och ändrade föreskrifterna och allmänna råden träder i kraft den 17 januari 2025.

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 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.

Innehållsförteckning

1 Utgångspunkter

Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 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 (Dora-förordningen) trädde i kraft den 17 januari 2023 och ska tillämpas från och med den 17 januari 2025. I förordningen finns enhetliga regler för de finansiella företagens[2] riskhantering när det gäller informations- och kommunikationsteknik (IKT), rapportering av IKT-relaterade incidenter, testning av företags digitala beredskap, riskhantering av tredjepartsleverantörer av IKT-tjänster samt informationsdelning. I Dora-förordningen anges att de europeiska tillsynsmyndigheterna inom ett flertal områden ska utarbeta förslag till tekniska standarder som kompletterar förordningen och som sedan ska beslutas av Europeiska kommissionen. Samtidigt som Dora-förordningen börjar gälla ändras även flera EU-direktiv på finansmarknadsområdet[3]. Ändringarna i de olika EU-direktiven syftar främst till att undvika dubbelreglering.

Dora-förordningen ska i vissa avseenden kompletteras av nationell lagstiftning. Riksdagen beslutade därför den 11 december 2024 lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn och ändringar i ett flertal rörelselagar på det finansiella området. Den nya lagstiftning som riksdagen beslutat om träder i kraft den 17 januari 2025, samtidigt som Dora-förordningen ska börja tillämpas i medlemsstaterna. De nya och ändrade föreskrifterna och allmänna råd som behandlas i denna promemoria träder i kraft vid samma tidpunkt.

Europaparlamentets och rådets förordning 600/2014/EU av den 15 maj 2014 om marknader för finansiella instrument (Mifir) har ändrats genom en förordning[4] som trädde i kraft den 28 mars 2024. Ändringarna innebär bland annat att två nya artiklar, som ställer krav på transparens före handel, har tillkommit. FI justerar därför i Finansinspektionens föreskrifter (FFFS

[2] I Dora-förordningen används begreppet ”finansiella entiteter”.
[3] Europaparlamentets och rådets direktiv (EU) 2022/2556 av den 14 december 2022 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.
[4] Europaparlamentet och rådets förordning (EU) 2024/791 av den 28 februari 2024 om ändring av förordning (EU) nr 600/2014 vad gäller att öka datatransparensen, undanröja hinder för framkomsten av konsoliderad handelsinformation, optimera handelsskyldigheterna och förbjuda mottagande av betalning av orderflöde.

2007:17) om verksamhet på marknadsplatser (marknadsplatsföreskrifterna), så att kraven på innehåll i den verksamhetsplan som företagen ska ge in vid en ansökan om tillstånd att bedriva börsverksamhet ligger i linje med ändringarna i Mifir.

1.1 Målet med regleringen

Det övergripande målet med FI:s verksamhet är att bidra till ett stabilt finansiellt system som präglas av ett högt förtroende med väl fungerande marknader som tillgodoser hushållens och företagens behov av finansiella tjänster samtidigt som det finns ett högt skydd för konsumenter.

När det handlar om att införa nya föreskrifter i anslutning till Dora-förordningen är målet med regleringen att möjliggöra för FI att dels på ett effektivt sätt ta emot de uppgifter som ska lämnas in enligt Dora-regelverket, dels vidarerapportera uppgifterna till de europeiska tillsynsmyndigheterna.

Målet med justeringarna i befintliga föreskrifter är huvudsakligen att undvika dubbelreglering, det vill säga att bestämmelser i FI:s föreskrifter och allmänna råd hamnar i konflikt med bestämmelser i Dora-förordningen, samt att hänvisningarna i föreskrifterna och de allmänna råden ska vara korrekta och språkbruket enhetligt. Till en begränsad del har ändringarna i föreskrifterna som mål att företagens verksamhetsplaner ska innehålla ytterligare information. Syftet med ändringarna är i den delen att säkerställa att företagens verksamhetsplaner återspeglar den verksamhet som bedrivs och innehåller relevant information om hur företagen uppfyller de krav som ställs i Mifir.

Sammantaget bidrar den nya regleringen till att FI kan uppfylla sitt övergripande mål för det finansiella systemet.

1.2 Nuvarande och kommande regelverk

De nya och ändrade föreskrifterna är en följd av Dora-förordningen och den kompletterande nationella lagstiftningen. Ändringarna i marknadsplatsföreskrifterna föranleds delvis av ändringar i Mifir.

Några ytterligare författningsändringar som påverkar de nya och ändrade föreskrifterna är inte kända i nuläget.

1.3 Regleringsalternativ

Ett alternativ till att införa nya föreskrifter är att lämna allmänna råd. Allmänna råd är dock till skillnad från föreskrifter inte bindande, utan är endast en rekommendation till företagen om hur de kan agera för att uppfylla de krav som ställs i lagar, förordningar eller myndighetsföreskrifter.

Bindande regler bedöms som det mest lämpliga alternativet när det gäller en ny reglering av formatet för rapportering av uppgifter till FI, eftersom samtliga institut är skyldiga att komma in med rapporteringen och FI i sin tur är skyldig att vidarebefordra informationen till den berörda europeiska tillsynsmyndigheten. Om företagen får välja vilka format de ska använda för att lämna uppgifter, kan FI inte vidarebefordra uppgifterna på något effektivt sätt.

Anpassningarna som FI föreslår till Dora-förordningen och till Mifir kräver att befintliga föreskrifter och allmänna råd ändras, vilket endast kan ske genom att ändringsföreskrifter meddelas och nya allmänna råd lämnas. Andra regleringsalternativ saknas därför i den delen.

1.4 Rättsliga förutsättningar

1.4.1 Förslaget till nya föreskrifter

Regeringen har den 12 december 2024 beslutat en ny förordning: förordningen (2024:1292) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn. I 2 § i den förordningen anges att FI får meddela föreskrifter om hur finansiella entiteter ska rapportera allvarliga IKT-relaterade incidenter enligt artikel 19.1 i Dora-förordningen, anmäla betydande cyberhot enligt artikel 19.2 i Dora-förordningen, och rapportera uppgifter om tredjepartsleverantörer av IKT-tjänster enligt artikel 28.3 i Dora-förordningen. I paragrafen ges FI också rätt att meddela föreskrifter om när dessa uppgifter ska lämnas.

Det är detta bemyndigande som FI stödjer sig på för att besluta de nya föreskrifterna om rapportering av incidenter och informationsregister enligt EU:s förordning om digital operativ motståndskraft för finanssektorn.

1.4.2 Ändringar av befintliga föreskrifter och allmänna råd

De föreskrifter och allmänna råd som anges nedan i punkterna a–m är sådana som ändras. Ändringarna innebär att vissa bestämmelser upphävs eller ändras för att undvika dubbelreglering, samt att vissa bestämmelser

tydliggörs i fråga om vad som behöver anges i en verksamhetsplan eller i rutiner till följd av Dora-förordningen eller Mifir. Nedan anges vilka bemyndiganden som FI stödjer sig på.

a) Finansinspektionens föreskrifter (FFFS 2007:17) om verksamhet på marknadsplatser, nedan *marknadsplatsföreskrifterna.* Bemyndigandena finns i 6 kap. 1 § 3, 4 och 7 förordningen (2007:572) om värdepappersmarknaden.
b) Finansinspektionens föreskrifter och allmänna råd (FFFS 2010:3) om betalningsinstitut och registrerade betaltjänstleverantörer, nedan *betaltjänstföreskrifterna*. Bemyndigandena finns i 5 § 1, 7, 17 och 19 förordningen (2010:1008) om betaltjänster.
c) Finansinspektionens föreskrifter och allmänna råd (FFFS 2011:49) om institut för elektroniska pengar och registrerade utgivare, nedan *e-pengaföreskrifterna*. Bemyndigandena finns i 6 § 2, 8, 9 och 11 förordningen (2011:776) om elektroniska pengar.
d) Finansinspektionens föreskrifter (FFFS 2013:9) om värdepappersfonder, nedan *värdepappersfondsföreskrifterna*. Bemyndigandena finns i 18 § 2 och 16 förordningen (2013:588) om värdepappersfonder.
e) Finansinspektionens föreskrifter (FFFS 2013:10) om förvaltare av alternativa investeringsfonder, nedan *AIF-förvaltarföreskrifterna*. Bemyndigandena finns i 4 § 4 och 5 § 12 förordningen (2013:587) om förvaltare av alternativa investeringsfonder.
f) Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut, nedan *SRK-föreskrifterna*. Bemyndigandet finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse.
g) Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker, nedan *föreskrifterna om operativa risker*. Bemyndigandena finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse.
h) Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem, nedan *it-föreskrifterna*. Bemyndigandet finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse och 6 kap. 1 § 33 förordningen (2007:572) om värdepappersmarknaden.
i) Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:13) om tillsynsrapportering för försäkringsrörelse, nedan *rapporteringsföreskrifterna för försäkringsrörelse*. Bemyndigandet finns i 7 kap. 2 § 60 försäkringsrörelseförordningen (2011:257).

j) Finansinspektionen föreskrifter och allmänna råd (FFFS 2018:4) om verksamhet för betaltjänstleverantörer, nedan *föreskrifterna om betaltjänstverksamhet*. Bemyndigandena finns i 5 § 13, 14 och 16 förordningen (2010:1008) om betaltjänster.
k) Finansinspektionens föreskrifter och allmänna råd (FFFS 2019:21) om tjänstepensionsföretag, nedan *tjänstepensionsföreskrifterna*. Bemyndigandet finns i 5 kap. 2 § 27 förordningen (2019:809) om tjänstepensionsföretag.
l) Finansinspektionens föreskrifter och allmänna råd (FFFS 2019:22) om tillsynsrapportering för tjänstepensionsföretag, nedan *rapporteringsföreskrifterna för tjänstepensionsföretag*. Bemyndigandet finns i 5 kap. 2 § 28 förordningen (2019:809) om tjänstepensionsföretag.
m) Finansinspektionens föreskrifter (FFFS 2024:5) om clearing och avveckling av betalningar, nedan *clearingföreskrifterna*. Bemyndigandet finns i 4 § 4 förordningen (2024:127) om clearing och avveckling av betalningar.

1.5 Ärendets beredning

Arbetet med att ta fram föreskrifterna och de allmänna råden påbörjades under våren 2023. FI höll den 26 april 2024 ett möte med en extern referensgrupp bestående av representanter från olika branschföreningar för företag som berörs av de planerade nya och ändrade föreskrifterna och allmänna råden. Vid mötet höll FI en presentation. Deltagarna fick därefter möjlighet att lämna synpunkter.

Den 4 september 2024 remitterade FI förslag till nya och ändrade föreskrifter och allmänna råd till 27 myndigheter, företag och organisationer. 16 remissinstanser har lämnat remissvar och 11 har avstått från att svara. Därutöver har ett yttrande inkommit från Livförsäkringsbolaget Skandia, ömsesidigt.

Den 21 november 2024 remitterade FI ett reviderat förslag till ikraftträdandebestämmelse till de nya föreskrifterna om rapportering av incidenter och informationsregister enligt EU:s förordning om digital operativ motståndskraft för finanssektorn (Dora-föreskrifterna). Remissen skickades till de remissinstanser som mottog den första remissen. Den 28 november 2024 höll FI ett särskilt remissmöte där remissinstanserna gavs möjlighet att muntligen framföra synpunkter på det reviderade förslaget till ikraftträdandebestämmelse. Sammanlagt 17 remissinstanser yttrade sig över tilläggsremissen, varav två deltog på det särskilda remissmötet.

Nedan redovisar och behandlar FI de remissynpunkter som kommit in.

2 Motivering och överväganden

FI beslutar att det ska införas nya föreskrifter (Dora-föreskrifterna) samt ändrar i ett antal befintliga föreskrifter och allmänna råd. I avsnitten 2.1–2.4 redovisar FI de nya och ändrade föreskrifterna och allmänna råden samt vilka överväganden som FI har gjort.

2.1 Nya föreskrifter med anledning av Dora-förordningen

Finansinspektionens ställningstagande: En ny föreskriftsbestämmelse införs om att sådana finansiella entiteter som avses i Dora-förordningen och som står under FI:s tillsyn ska rapportera allvarliga IKT-relaterade incidenter och betydande cyberhot till FI på det sätt som anges på FI:s webbplats. Det införs också en ny föreskriftsbestämmelse om hur och när de finansiella entiteterna ska ge FI tillgång till sitt fullständiga register med information om kontraktsmässiga arrangemang enligt artikel 28.3 fjärde stycket i Dora-förordningen. De finansiella entiteterna ska göra det genom att lämna in sitt fullständiga informationsregister till FI senast den 28 februari varje år på det sätt som anges på FI:s webbplats. Den version av registret som lämnas in ska avse förhållandena vid utgången av föregående kalenderår.

Remisspromemorian: Förslaget hade samma innehåll i sak. Föreskriftsbestämmelsen om inlämnande av informationsregister har dock justerats för att förtydliga att den avser de finansiella entiteternas skyldighet enligt Dora-förordningen att ge den behöriga myndigheten tillgång till sina fullständiga informationsregister.

Remissinstanserna: *Tjänstepensionsförbundet* anser att det inte motiveras tillräckligt i remisspromemorian varför FI begär att få in ett fullständigt informationsregister varje år och att sådan årlig rapportering borde föranleda att rapportering enligt artikel 28.3 tredje stycket i Dora-förordningen inte behövs. *Svenska Bankföreningen* anser att förslagets formulering gör det oklart om den årliga rapporteringen avser det fullständiga informationsregistret eller endast förändringar i registret. *Sparbankernas Riksförbund* och *Svenska Pensionsstiftelsers Förening (SPFA)* anser att en årlig rapportering av fullständigt register går längre än vad Dora-förordningen kräver.

SPFA efterfrågar en tydligare motivering av varför ett sådant krav är nödvändigt, och anser att kravet bör begränsas till att endast gälla aktörer av viss storlek alternativt om särskild anledning föranleder rapportering. SPFA menar vidare att rapporteringen bör begränsas till information om nya arrangemang. *Livförsäkringsbolaget Skandia, ömsesidigt (Skandia)* anser att artikel 28.3 fjärde stycket i Dora-förordningen inte är en bestämmelse om årlig rapportering av det fullständiga informationsregistret och att det angivna bemyndigandet endast avser nya arrangemang. Bolaget efterfrågar ett förtydligande om FI menar att det fullständiga informationsregistret ska rapporteras årligen, och i sådant fall ett förtydligande av om företagen därutöver förväntas rapportera om nya avtal enligt artikel 28.3 tredje stycket i Dora-förordningen. *Finansbolagens förening* anför att ett fullständigt register ska lämnas in på begäran av den behöriga myndigheten och att det inte är nödvändigt att uttrycka en sådan begäran i föreskrifter. *Swedish Financial Benchmark Facility AB (SFBF)* anser att det finns en rad otydligheter avseende format och tillvägagångssätt vid rapportering, särskilt för finansiella entiteter som inte har tidigare erfarenhet av sedvanlig rapportering till FI eller som inte varit delaktiga i de europeiska tillsynsmyndigheternas testperiod för rapportering av informationsregister. Vidare efterfrågar SFBF att FI skyndsamt publicerar teknisk information om rapporteringen samt möjliggör för berörda företag att i tid implementera lösningar, ställa frågor och erhålla stöd i rapporteringsrelaterade frågor. Finansbolagens förening efterfrågar ett förtydligande av om finansiella institut som inte omfattas av Dora-förordningens tillämpningsområde men som står under FI:s tillsyn ska rapportera incidenter enligt Dora-förordningen. *Sveriges advokatsamfund* efterfrågar tolkningar av olika aspekter i artikel 28.3 i Dora-förordningen, samt vägledning kring relationen mellan särskilda riktlinjer från Europeiska värdepappersmarknadsmyndigheten och Dora-regelverkets rapporteringskrav. Sparbankernas Riksförbund anser att det är olyckligt att proportionalitetsprincipen inte beaktats mer och refererar till artikel 28.10 i Dora-förordningen samt till det regelförenklingsuppdrag som regeringen gett ett flertal myndigheter i deras regleringsbrev. SPFA efterfrågar en tydligare redogörelse för de överväganden som gjorts kring ökad administrativ och regulatorisk börda, samt risker, som förslaget kan medföra för de finansiella entiteterna.

Finansinspektionens skäl: Rapportering av IKT-relaterade incidenter och informationsregister är en central del av regleringen i Dora-förordningen. Tanken är att de europeiska tillsynsmyndigheterna ska få en samlad bild av IKT-relaterade incidenters art, frekvens, betydelse och inverkan. I syfte att

skapa en enhetlig rapportering av incidenter finns bestämmelser i artikel 19.1 fjärde stycket i Dora-förordningen om att sådan rapportering ska göras enligt de mallar som beslutats enligt artikel 20 i Dora-förordningen.

Av artikel 28.3 i Dora-förordningen följer att de finansiella entiteterna på begäran av den behöriga myndigheten ska ge myndigheten tillgång till sitt fullständiga informationsregister, eller särskilt angivna delar av det. Europeiska kommissionen har den 29 november 2024 fattat beslut om en genomförandeförordning (en så kallad teknisk standard för genomförande) som fastställer de mallar som ska användas för rapportering av informationsregister enligt artikel 28.3.

De uppgifter som FI får genom incidentrapportering och rapportering av informationsregister ska FI vidareförmedla i ett visst format till de EU-institutioner som anges i Dora-förordningen. Det är därför av vikt att FI som behörig myndighet får in rapportering i det format som anvisas av de europeiska tillsynsmyndigheterna, så att en snabb och felfri informationsöverföring kan ske.

FI anser därför att företagen bör lämna in den nämnda rapporteringen på det sätt som anges på FI:s webbplats, och att det formatet även ska användas vid frivillig anmälan av betydande cyberhot enligt artikel 19.2 i Dora-förordningen. En ny föreskriftsbestämmelse införs av den innebörden. Det format som anges på FI:s webbplats kommer att stämma överens med det format som de europeiska tillsynsmyndigheterna anvisar de behöriga myndigheterna att använda vid vidarerapporteringen. FI har ännu inte erhållit besked om på vilket sätt som rapporteringen ska göras, men kommer att publicera den informationen på FI:s webbplats så snart den finns tillgänglig.

De nya bestämmelserna om rapportering enligt Dora-förordningen samlas i en ny författning, Dora-föreskrifterna. När det gäller vilka företag som ska tillämpa föreskrifterna, en fråga som *Finansbolagens förening* tar upp, så är kraven i 2 § kumulativa. Detta innebär att föreskrifterna ska tillämpas på finansiella entiteter som både omfattas av artikel 2 i Dora-förordningen och som står under FI:s tillsyn.

De europeiska tillsynsmyndigheterna fattade den 8 november 2024 beslut om att de behöriga myndigheterna, dvs. bland annat FI, senast den 31 mars varje år till dem ska vidarebefordra de informationsregister som företagen

har lämnat in.[5] De europeiska tillsynsmyndigheternas beslut har fattats med stöd av deras inrättandeförordningar[6], i synnerhet artikel 35 i förordningarna, och är bindande för FI som behörig myndighet. Uppgifterna i informationsregistren ska ligga till grund för de europeiska tillsynsmyndigheternas beslut om kritiska tredjepartsleverantörer enligt Dora-förordningen.

Av samma beslut framgår att rapporteringen av informationsregister ska avse förhållandena vid utgången av föregående kalenderår. Vidare anges det i beslutet vid vilken tidpunkt som informationsregistren ska vidarebefordras första gången, det vill säga under 2025. Frågan om rapporteringstidpunkter under 2025 behandlas i avsnitt 2.4 i denna beslutspromemoria.

Tjänstepensionsförbundet, *Svenska Bankföreningen* och *Skandia* har tagit upp frågan om det är det fullständiga informationsregistret som ska rapporteras in årligen till Finansinspektionen, eller om det endast är information om nya arrangemang enligt artikel 28.3 tredje stycket som ska lämnas in. Som framgår ovan har de europeiska tillsynsmyndigheterna fattat beslut om att de behöriga myndigheterna, däribland FI, ska vidarebefordra företagens informationsregister till de europeiska tillsynsmyndigheterna senast den 31 mars varje år. I skälssatserna i det beslutet anges att de behöriga myndigheterna ska använda sig av befogenheten enligt artikel 28.3 fjärde stycket i Dora-förordningen att begära att få tillgång till de finansiella entiteternas fullständiga informationsregister. Det är därför det fullständiga informationsregistret som ska lämnas in årligen, inte endast information om nya arrangemang.

Finansbolagens förening, Skandia, *SPFA* och *Sparbankernas Riksförbund* har ifrågasatt om FI har möjligheter enligt Dora-förordningen att begära in

[5] Decision of the European Banking Authority, Decision of the European Securities and Markets Authority, Decision of the European Insurance and Occupational Pensions Authority of 08 November 2024 concerning the reporting by competent authorities to the ESAs of information necessary for the designation of critical ICT third-party service providers in accordance with Article 31(1)(a) of Regulation (EU) 2022/2554 (ESA 2024 22)

[6] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten, samt Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten).

det fullständiga informationsregistret årligen, om det är nödvändigt att ställa ett sådant krav i föreskrifter och vilket bemyndigande som myndigheten har.

I bemyndigandet i 2 § 3 förordningen (2024:1292) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn anges att FI får meddela föreskrifter om hur och när rapportering av uppgifter om tredjepartsleverantörer av IKT-tjänster ska göras enligt artikel 28.3 i EU-förordningen. I artikel 28.3 fjärde stycket, dvs. i den artikel som omnämns i bemyndigandet, anges att de finansiella entiteterna på begäran ska ge den behöriga myndigheten tillgång till det fullständiga informationsregistret. Mot denna bakgrund anser FI att det nämnda bemyndigandet ger FI stöd för att meddela föreskrifter av den innebörden att de finansiella entiteter enligt Dora-förordningen som står under FI:s tillsyn årligen ska lämna in ett fullständigt informationsregister. Att sådan årlig rapportering sker är också nödvändigt för att FI ska kunna följa de europeiska tillsynsmyndigheternas beslut.

FI inför därför en föreskriftsbestämmelse i vilken det anges att en finansiell entitet ska ge Finansinspektionen tillgång till sitt fullständiga register med information om kontraktsmässiga arrangemang enligt artikel 28.3 fjärde stycket i Dora-förordningen genom att årligen lämna in registret till Finansinspektionen.

För att FI ska kunna följa det beslutet och senast den 31 mars varje år vidarebefordra informationsregistren till de europeiska tillsynsmyndigheterna krävs att företagen lämnar in sitt fullständiga informationsregister till FI senast den 28 februari varje år. Detta bedöms ge FI tillräckligt med tid för att säkerställa en korrekt överföring till de europeiska myndigheterna. En sådan skyldighet införs därför i den nya föreskriftsbestämmelsen.

I och med att det fullständiga informationsregistret ska lämnas in varje år kommer även de nya kontraktsmässiga arrangemang som har tillkommit under det gångna året att finnas med i det inlämnade informationsregistret. Företagen behöver därför inte lämna någon särskild information om nya arrangemang enligt artikel 28.3 tredje stycket i Dora-förordningen, en fråga som Tjänstepensionsförbundet och Skandia berört.

FI noterar att vissa remissinstanser har efterlyst vägledning, tolkning och utbildningstillfällen om Dora-förordningen. Detta är dock frågor som faller utanför ramen för detta regelärende. FI noterar dock att de europeiska

tillsynsmyndigheterna erbjuder vissa utbildningstillfällen som företagen kan delta i.

2.2 De allmänna råden om rapportering av händelser av väsentlig betydelse ändras

Finansinspektionens ställningstagande: Den incidentrapportering som ska ske enligt Dora-förordningen ska inte omfattas av Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse. Därför lämnas nya allmänna råd om rapportering av händelser av väsentlig betydelse vars tillämpningsområde inte omfattar incidentrapportering enligt Dora-förordningen.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Finansbolagens förening* och *Fondbolagens förening* önskar se ett förtydligande av vad som ska rapporteras enligt Dora-förordningen respektive enligt de allmänna råden i fråga om ”fel uppstår i tekniska system”. *Sparbankernas riksförbund* anser att det finns skäl att se över och förtydliga de allmänna råden när det gäller dels vilken funktion på företaget som lämnar en rapport, dels vad gäller anmälan om misstanke om brott.

Finansinspektionens skäl: I Finansinspektionens allmänna råd (FFFS 2021:2) om rapportering av händelser av väsentlig betydelse finns bland annat allmänna råd om att företag under myndighetens tillsyn bör rapportera när vissa händelser inträffar i verksamheten. Det handlar om händelser som kan äventyra företagens stabilitet eller skyddet av kundernas tillgångar, vilket exempelvis inkluderar att fel uppstår i tekniska system.

Genom Dora-förordningen införs krav på IKT-relaterad incidentrapportering (Kapitel III i Dora-förordningen). För att undvika dubbelrapportering bör de allmänna råden om rapportering av händelser av väsentlig betydelse inte gälla för sådan incidentrapportering som ska ske enligt Dora-förordningen. FI beslutar därför att Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse ska ersättas av nya allmänna råd som inte gäller för IKT-relaterad incidentrapportering enligt Dora-förordningen. De allmänna råden ska alltjämt tillämpas för rapportering av andra händelser av väsentlig betydelse än de som omfattas av Dora-förordningen.

Vilka incidenter som omfattas av Dora-förordningen måste avgöras genom en tolkning av den förordningen, som inspektionen inte kan göra i de allmänna råden. FI kan därför inte tillgodose önskemålet om förtydligande från *Finansbolagens förening* och *Fondbolagens förening*. Det är dock svårt att tänka sig att ett företag som har lämnat en rapport om fel i tekniska system enligt de mallar som ska användas för incidentrapportering enligt Dora-förordningen skulle agera i strid med de nu behandlade allmänna råden.

I detta regelärende behandlas endast sakliga förändringar i de allmänna råden som hänger samman med att Dora-förordningen ska börja tillämpas. Att förtydliga de allmänna råden i enlighet med önskemålet från *Sparbankernas Riksförbund*, när det gäller vilken funktion på ett företaget som ska lämna en rapport och ansvaret för att göra en anmälan om misstanke om brott, faller därför utanför ramen för ärendet.

2.3 Ändringar i befintliga föreskrifter och allmänna råd

2.3.1 Marknadsplatsföreskrifterna

Finansinspektionens ställningstagande: Ett företag ska i sin verksamhetsplan särskilt ange hur det ska följa Dora-förordningen. I verksamhetsplanen ska det också finnas en beskrivning av sådana arrangemang, planer, förfaranden och mekanismer som företaget har fastställt för att säkerställa att information om allvarliga IKT-relaterade incidenter och betydande cyberhot överförs till en behörig myndighet enligt artikel 19 i Dora-förordningen. I sin verksamhetsplan ska ett företag dessutom redogöra för hur det uppfyller reglerna i artiklarna 8 a och 8 b i Mifir, som ställer krav på transparens före handel på handelsplatser när det gäller derivat respektive paketorder.

Därutöver görs vissa redaktionella ändringar av föreskrifterna.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De remissinstanser som har yttrat sig har inte haft några synpunkter på förslaget.

Finansinspektionens skäl: Marknadsplatsföreskrifterna gäller för bland annat börser och värdepappersinstitut, vilka också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 e och i). De föreskrifterna behöver därför anpassas så att den verksamhetsplan som lämnas in i sam-

band med en ansökan innehåller uppgifter om hur företaget ska uppfylla vissa krav i Dora-förordningen.

FI inför en hänvisning till Dora-förordningen i 1 a kap. för att förtydliga att uppgifterna som ett företag ska lämna i sin verksamhetsplan om hur det ska styra och följa upp sitt it-säkerhetsarbete, särskilt ska omfatta hur företaget följer kraven i Dora-förordningen.

FI inför vidare en ny bestämmelse som ställer krav på att ett företags verksamhetsplan ska beskriva eventuella arrangemang, planer, förfaranden och mekanismer som företaget har fastställt för att säkerställa att information om allvarliga IKT-relaterade incidenter och betydande cyberhot överförs till behörig myndighet i enlighet med Dora-förordningen. Bestämmelsen införs eftersom nuvarande 1 a kap. 21 § – som visserligen ställer motsvarande krav – innehåller en hänvisning till de allmänna råden (FFFS 2021:2) om rapportering av händelser av väsentlig betydelse. Eftersom dessa allmänna råd ändras och ges ut på nytt, och framöver inte ska gälla för incidentrapportering enligt Dora-förordningen, behöver ett krav införas i marknadsplatsföreskrifterna på att en verksamhetsplan ska beskriva rutiner för incidentrapportering enligt Dora-förordningen.

Eftersom nya allmänna råd beslutas för rapportering av händelser av väsentlig betydelse, görs även en justering av 1 a kap. för att marknadsplatsföreskrifterna ska hänvisa korrekt.

Enligt 1 a kap. 28 § marknadsplatsföreskrifterna ska den verksamhetsplan som ett företag ska lämna in vid en ansökan om tillstånd att bedriva börsverksamhet innehålla en redogörelse för hur företaget uppfyller reglerna om information före och efter handel i artiklarna 3, 6, 8 och 10 i Mifir. Som en konsekvens av att fler artiklar om transparens före handel har tillkommit i Mifir, ändras 1 a kap. 28 § så att den verksamhetsplan som ska ges in i samband med en ansökan om tillstånd även ska innehålla en redogörelse som omfattar de nya artiklarna 8a och 8b i Mifir. Därmed återspeglar en ansökan om tillstånd de krav som ställs på verksamheten enligt Mifir.

2.3.2 Betaltjänstföreskrifterna

Finansinspektionens ställningstagande: Ett företag ska i sin verksamhetsplan ange hur det följer Dora-förordningen. Beskrivningen i verksamhetsplanen av företagets system för hantering av operativa risker och säkerhetsrisker ska omfatta företagets rutiner för att underrätta Finansinspektionen

om allvarliga operativa incidenter och säkerhetsincidenter enligt artikel 19 i Dora-förordningen.

Bestämmelserna i betaltjänstföreskrifterna om uppdragsavtal ska inte gälla för sådana uppdragsavtal som omfattas av i Dora-förordningens bestämmelser om hantering av IKT-tredjepartsrisker (Kapitel V).

Upplysningsbestämmelsen om rapportering av allvarliga operativa incidenter och säkerhetsincidenter i betaltjänstverksamhetsföreskrifterna upphävs.

Det införs en definition av Dora-förordningen.

Därutöver görs redaktionella ändringar.

Remisspromemorian: Förslaget hade i sak samma innehåll, men vissa redaktionella ändringar görs i förhållande till det remitterade förslaget.

Remissinstanserna: De remissinstanser som har yttrat sig har inte haft några synpunkter på förslaget.

Finansinspektionens skäl: Betaltjänstföreskrifterna gäller för betalningsinstitut och registrerade betaltjänstleverantörer, som också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 b). De föreskrifterna anpassas därför så att de inte står i strid med Dora-förordningen.

I den verksamhetsplan som ett företag enligt 2 kap. 16 och 16 a §§ ska ge in samband med en ansökan om tillstånd, ska företaget ange hur it-verksamheten för betaltjänster är organiserad samt beskriva sitt system och sina rutiner för hantering av operativa risker. För att tydliggöra att verksamhetsplanen även ska innehålla information om hur ett företag uppfyller kraven i Dora-förordningen, inför FI en hänvisning till förordningen i de nämnda paragraferna.

I 10 kap. finns bestämmelser om uppdragsavtal som är av väsentlig betydelse för betaltjänstverksamheten. Bland annat anges att uppdrag ska regleras i skriftliga avtal samt hur utformningen av dessa avtal ska vara. I kapitel V i Dora-förordningen finns bestämmelser om hantering av risker som kan uppstå i samband med att ett företag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör. De bestämmelserna innehåller krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering ska 10 kap. inte

gälla för sådana uppdragsavtal som regleras i Dora-förordningen. FI anser därför att 10 kap. ska kompletteras med en bestämmelse om att kapitlet inte ska tillämpas på uppdragsavtal som omfattas av kapitel V i Dora-förordningen. Kapitlet ska alltjämt tillämpas på andra uppdragsavtal än de som omfattas av Dora-förordningen.

12 kap. 4 § ska upphöra att gälla, eftersom den innehåller en upplysning om att bestämmelser om rapportering av allvarliga operativa incidenter och säkerhetsincidenter för betalningsinstitut och registrerade betaltjänstleverantörer finns i 6 kap. 4 § föreskrifterna om betaltjänstverksamhet. Eftersom den sistnämnda bestämmelsen upphör att gälla (se avsnitt 2.3.9), behöver även 12 kap. 4 § i de nu aktuella föreskrifterna tas bort.

En definition av Dora-förordningen införs i det inledande kapitlet, eftersom hänvisningar till Dora-förordningen läggs till på ett antal ställen i föreskrifterna.

2.3.3 E-pengaföreskrifterna

Finansinspektionens ställningstagande: E-pengaföreskrifternas bestämmelser om verksamhetsplanens innehåll i fråga om it-verksamhet och rutiner för rapportering av händelser av väsentlig betydelse kompletteras med en hänvisning till Dora-förordningen.

Bestämmelserna i e-pengaföreskrifterna om uppdragsavtal ska inte gälla för sådana uppdragsavtal som omfattas av Dora-förordningens bestämmelser om hantering av IKT-tredjepartsrisker (Kapitel V).

Upplysningsbestämmelsen om regleringen i betaltjänstverksamhetsföreskrifterna om rapportering av allvarliga operativa incidenter och säkerhetsincidenter upphävs.

Det införs en definition av Dora-förordningen i föreskrifterna.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De remissinstanser som har yttrat sig har inte haft några synpunkter på förslaget.

Finansinspektionens skäl: E-pengaföreskrifterna gäller för institut för elektroniska pengar och registrerade utgivare av elektroniska pengar, som också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 d). De

föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

För att tydliggöra att den verksamhetsplan som ska lämnas in i samband med en ansökan om tillstånd att ge ut elektroniska pengar ska innehålla uppgifter om hur ett företag följer Dora-förordningen, inför FI ett tillägg som reglerar vad en sådan verksamhetsplan ska innehålla (2 kap. 15 §). Vidare ska företaget i verksamhetsplanen redogöra för vilka rutiner det har för att rapportera betalningsrelaterade operativa incidenter och säkerhetsincidenter enligt artikel 19 i Dora-förordningen. Tillägget görs i den bestämmelse i e-pengaföreskrifterna (2 kap. 21 §) som behandlar rutiner för rapportering av händelser av väsentlig betydelse.

I 8 kap. finns bestämmelser om uppdragsavtal som är av väsentlig betydelse för verksamheten. Bland annat föreskrivs där att uppdrag ska regleras i skriftliga avtal och det finns bestämmelser om hur dessa avtal ska utformas. I kapitel V i Dora-förordningen finns bestämmelser om hantering av risker som kan uppstå i samband med att ett företag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör inklusive krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30.

För att undvika dubbelreglering ska 8 kap. inte gälla för sådana uppdragsavtal som regleras i Dora-förordningen. FI beslutar därför att 8 kap. ska kompletteras med en bestämmelse som klargör att kapitlet inte ska tillämpas på uppdragsavtal som omfattas av kapitel V i Dora-förordningen. 8 kap. ska alltjämt tillämpas på andra uppdragsavtal än de som omfattas av Dora-förordningen.

10 kap. 4 a § upphör att gälla, eftersom den innehåller en upplysning om att bestämmelser om rapportering av allvarliga operativa incidenter och säkerhetsincidenter för institut för elektroniska pengar och registrerade utgivare finns i 6 kap. 4 § föreskrifterna om betaltjänstverksamhet. Eftersom den sistnämnda bestämmelsen upphör att gälla (se avsnitt 2.3.9), ska även 10 kap. 4 a § i de nu aktuella föreskrifterna tas bort.

Eftersom det införs hänvisningar till Dora-förordningen på ett antal ställen i föreskrifterna, införs även en definition av förordningen i det inledande kapitlet.

2.3.4 Värdepappersfondföreskrifterna

Finansinspektionens ställningstagande: Ett fondbolag ska i sin verksamhetsplan redogöra för hur det säkerställer att det uppfyller Dora-förordningens bestämmelser om hantering av IKT-tredjepartsrisker (Kapitel V).

Bestämmelsen om att ett fondbolag ska ha aktuella system och rutiner för att skydda säkerhet, integritet och konfidentialitet i sin information upphävs.

Bestämmelserna i föreskrifterna om rapportering av händelser av väsentlig betydelse ska inte gälla för incidentrapportering enligt artikel 19 i Dora-förordningen. Bestämmelserna om uppdragsavtal i 14 kap. i föreskrifterna ska inte gälla för sådana uppdragsavtal som rör hantering av IKT-tredjepartsrisker enligt kapitel V i Dora-förordningen.

Det införs en definition av Dora-förordningen i föreskrifterna. Vidare görs vissa redaktionella ändringar.

Remisspromemorian: Förslaget hade i sak samma innehåll, dock görs vissa redaktionella ändringar i förhållande till det remitterade förslaget.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Fondbolagens förening* önskar att FI dels ska förtydliga vad som avses med ”i god tid” i artikel 28.3 femte stycket i Dora-förordningen, dels klargöra vilken tidsfrist som gäller för inlämnande av IKT-avtal. Föreningen anser också att det bör klargöras om de finansiella entiteterna för IKT-avtalen ska tillämpa enmånadsregeln enligt 3 kap. 1 § fondföreskrifterna eller bestämmelsen om ”i god tid” enligt Dora-förordningen.

Finansinspektionens skäl: Värdepappersfondföreskrifterna gäller för fondbolag, som också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 l). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

Ett tillägg görs i bestämmelserna om ett fondbolags verksamhetsplan, av den innebörden att det ska framgå av verksamhetsplanen hur ett företag uppfyller kraven i Dora-förordningen på hantering av IKT-tredjepartsrisker.

FI beslutar att bestämmelserna om vad en verksamhetsplan ska innehålla i fråga om uppdragsavtal och it-verksamhet (2 kap. 11 och 12 §§) ska kompletteras med hänvisningar till Dora-förordningen för att tydliggöra att även

uppgifter enligt denna förordning ska ingå. Hänvisningarna till Dora-förordningen är fördelade på två olika bestämmelser, för att följa den uppdelning som redan finns i föreskrifterna (uppdragsavtal respektive it-verksamhet).

Bestämmelserna om skydd för säkerhet, integritet och konfidentialitet i ett fondbolags information i 7 kap. 2 § har en motsvarighet i artiklarna 6 och 9 i Dora-förordningen. Detta innebär en dubbelreglering i förhållande till Dora-förordningen, varför FI beslutar att bestämmelsen ska upphöra att gälla.

Kraven i 7 kap. 19 § sista meningen om säkerhet i fråga om elektronisk databehandling och uppgifters integritet och konfidentialitet, motsvaras av artiklarna 6, 7 och 9 i Dora-förordningen. Detta innebär en dubbelreglering i förhållande till Dora-förordningen, varför FI beslutar att den angivna meningen ska tas bort.

I 10 kap. i värdepappersfondsföreskrifterna finns bestämmelser om rapportering av händelser av väsentlig betydelse. Det är fråga om händelser som kan äventyra bolagets stabilitet, skyddet av kundernas tillgångar eller som innebär att bolaget inte kan uppfylla sina åtaganden mot kunder. På samma sätt som för de allmänna råden om rapportering av händelser av väsentlig betydelse (se avsnitt 2.3 ovan) uppstår en dubbelreglering i förhållande till Dora-förordningen. FI beslutar därför att det i 10 kap. ska anges att kapitlet inte ska gälla för sådana allvarliga IKT-incidenter som omfattas av artikel 19 i Dora-förordningen. 10 kap. ska alltjämt tillämpas för rapportering av andra händelser av väsentlig betydelse än de som omfattas av Dora-förordningen.

I 14 kap. i värdepappersfondföreskrifterna finns bestämmelser om uppdragsavtal. Bland annat innehåller kapitlet bestämmelser om att uppdrag ska regleras i skriftliga avtal och om utformningen av dessa avtal. I kapitel V i Dora-förordningen finns bestämmelser om hantering av risker som kan uppstå i samband med att ett företag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör inbegripet krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering ska 14 kap. inte gälla för sådana uppdragsavtal som regleras i Dora-förordningen. 14 kap. ska alltjämt tillämpas för andra uppdragsavtal än de som omfattas av Dora-förordningen.

Fondbolagens förening efterlyser ett förtydligande av vad som ska anses vara god tid enligt artikel 28.3 femte stycket Dora-förordningen. Vidare tar föreningen tar upp frågan om huruvida 3 kap. 1 § i värdepappersfonds-

föreskrifterna hamnar i konflikt med Dora-förordningen. Bestämmelsen i 3 kap. 1 § i värdepappersfondföreskrifterna kompletterar 4 kap. 7 § lagen (2004:46) om värdepappersfonder, och gäller för uppdragsavtal som avser fondförvaltning eller därmed sammanhängande administration. För uppdragsavtal som avser IKT-tjänster gäller Dora-förordningen.

FI kan inte påverka innehållet i vare sig lagen om värdepappersfonder eller Dora-förordningen. Inte heller kan FI i inom ramen för detta regelärende uttala sig om tolkningen av begreppen ”god tid” eller ”kontraktsmässigt arrangemang om användning av IKT-tjänster” i Dora-förordningen. Därför kan några sådana förtydliganden som Fondbolagens förening efterlyser inte lämnas.

Eftersom en hänvisning till Dora-förordningen görs på ett antal ställen i föreskrifterna, införs en definition av förordningen i det inledande kapitlet.

2.3.5 AIF-förvaltarföreskrifterna

Finansinspektionens ställningstagande: Redogörelsen för uppdragsavtal i en AIF-förvaltares verksamhetsplan ska även innehålla uppgifter om hur förvaltaren säkerställer att den uppfyller kraven på uppdragsavtal i Dora-förordningen. I verksamhetsplanen ska en AIF-förvaltare därutöver även beskriva hur AIF-förvaltaren uppfyller de krav som följer av Dora-förordningen när det gäller organisation av it-verksamheten.

Vidare inför FI en definition av Dora-förordningen i föreskrifterna. Även vissa redaktionella ändringar görs i föreskrifterna.

Remisspromemorian: Förslaget hade i sak samma innehåll. Vissa redaktionella och språkliga ändringar görs i förhållande till det remitterade förslaget.

Remissinstanserna: De remissinstanser som har yttrat sig har inte haft några synpunkter på förslaget.

Finansinspektionens skäl: AIF-förvaltarföreskrifterna gäller för AIF-förvaltare, som också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 k). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

Det är lämpligt att en AIF-förvaltares verksamhetsplan även innehåller en redogörelse för hur förvaltaren följer kraven i Dora-förordningen i fråga om uppdragsavtal och it-verksamhet (3 kap. 16 och 17 §§). De paragraferna

kompletteras därför med hänvisningar till Dora-förordningen. Hänvisningarna till Dora-förordningen är fördelade på två olika bestämmelser, för att följa den uppdelning i ämnesområden som redan finns i föreskrifterna (uppdragsavtal respektive it-verksamhet).

Eftersom hänvisningar görs till Dora-förordningen på ett antal ställen i föreskrifterna, införs även en definition av förordningen i det inledande kapitlet.

2.3.6 SRK-föreskrifterna

Finansinspektionens ställningstagande: Bestämmelserna i föreskrifterna om allmänna organisatoriska krav, styrelsens och verkställande direktörens ansvar och riskhantering (2, 3 och 5 kap.) ska inte gälla för hantering av IKT-risker enligt Dora-förordningen. Bestämmelserna om uppdragsavtal (10 kap.) ska inte gälla för sådana uppdragsavtal som omfattas av Dora-förordningen.

Bestämmelserna om att företag ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i sin information (2 kap. 2 §) ska upphöra att gälla.

Bestämmelsen om riskhantering i samband med större förändringar (5 kap. 4 §) ska inte längre gälla vid införandet av nya eller väsentligt förändrade it-system.

Det ska införas en definition av Dora-förordningen i föreskrifterna och vissa redaktionella ändringar ska göras.

Remisspromemorian: Förslaget hade samma innehåll i sak men var något annorlunda utformat i redaktionellt hänseende.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Svenska Bankföreningen* anför att 2 kap. 3 § bör korrigeras eftersom det anges där att företag ska ha en dokumenterad riskaptit som omfattar alla slag av risker, vilket är motsägelsefullt då föreskrifterna inte avses gälla för IKT-risker enligt Dora-förordningen. Bankföreningen har också synpunkter på huruvida bestämmelsen i 2 kap. 9 § om kontinuitetshantering är förenlig med de krav som uppställs i artiklarna 11 och 12 i Dora-förordningen. Svenska Bankföreningen anför vidare att bestämmelsen om riskhantering vid förändringar i 5 kap. 4 § är svår att tolka och att det inte stämmer att motsvarande krav återfinns i art 6, 7 och 8.3 i Dora-förordningen. Vidare efterfrågar föreningen att FI på paragrafnivå

anger vilka krav i Dora-förordningen som motsvarar en paragraf i SRK-föreskrifterna. Därutöver påtalar Svenska Bankföreningen att begreppet ”it-system” inte har tagits bort från 7 kap. 3 § 9 och 8 kap. 3 § 5 i SRK-föreskrifterna. Avslutningsvis efterfrågar Svenska Bankföreningen och *Sparbankernas riksförbund* ett förtydligande av hur begreppet ”alla väsentliga risker” i 7 kap. 3 § ska tolkas, eftersom det i föreskrifterna införs en begränsning som innebär att IKT-risker inte omfattas av dem.

Finansinspektionens skäl: SRK-föreskrifterna gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag och kreditmarknadsföreningar som i egenskap av kreditinstitut också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 a). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

För att anpassa föreskrifterna så att de inte står i strid med Dora-förordningen krävs att sådana bestämmelser i föreskrifterna som har ett innehåll som också finns i Dora-förordningen stryks. Nationella bestämmelser får inte reglera något som regleras i Dora-förordningen.

De förändringar som införs innebär att det är Dora-förordningen som gäller för hantering av IKT-risker, medan SRK-föreskrifterna fortsatt gäller för hanteringen av övriga typer av risker som omfattas av de föreskrifterna. Det ankommer inte på FI att inom ramen för detta regelärende närmare redogöra för hur Dora-förordningen ska tolkas i olika avseenden, utan endast att förklara varför vissa krav tas bort eller begränsas när det i Dora-förordningen finns krav som rör samma sak. FI kan inte heller, som *Svenska Bankföreningen* efterfrågar, på paragrafnivå förtydliga förhållandena mellan SRK-föreskrifterna och Dora-förordningen, utöver det som FI i denna beslutspromemoria uttalar om de ändringar som görs i syfte att undvika dubbelreglering.

Bestämmelsen i 2 kap. 2 § i föreskrifterna ska upphöra att gälla, Paragrafen innehåller krav på att företag ska ha ändamålsenliga it-system och rutiner. I artiklarna 7 och 9 i Dora-förordningen finns bland annat krav på att företagens IKT-system ska vara uppdaterade, tillförlitliga, tekniskt motståndskraftiga och hålla höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet avseende data. De nämnda kraven i Dora-förordningen har i allt väsentligt samma sakliga innehåll som 2 kap. 2 § i föreskrifterna, varför den bestämmelsen bör utgå.

FI inför en begränsning av tillämpningsområdet för 2 kap. som innebär att föreskrifterna inte gäller för sådan hantering av IKT-risker som avses i Dora-förordningen. De krav som anges i 2 kap. i föreskrifterna överlappar delvis med kapitel II i Dora-förordningen, särskilt artiklarna 7–9. För att undvika dubbelreglering införs en begränsning i föreskrifternas tillämpningsområde såvitt gäller hantering av IKT-risker. Kapitlets tillämpningsområde i övrigt förändras inte. När det gäller kraven i 2 kap. 3 och 9 §§ på att företagen ska ha en dokumenterad riskaptit respektive en väl fungerande kontinuitetshantering, som *Svenska Bankföreningen* lyfter fram i sitt remissvar, innebär den begränsning som införs i fråga om hantering av IKT-risker att företagen i dessa avseenden ska följa Dora-förordningen. Eftersom det i Dora-förordningen finns bestämmelser om företagens IKT-riskhanteringsram, som omfattar såväl riskaptit som kontinuitetshantering, kan SRK-föreskrifterna inte innehålla bestämmelser om samma sak.

Bestämmelserna i 3 kap. i SRK föreskrifterna behandlar styrelsens och den verkställande direktörens ansvar. Kapitlet tar bland annat upp styrelsens ansvar över strategier och uppdatering av interna regler. Kapitel II i Dora-förordningen innehåller bestämmelser vilkas tillämpningsområde överlappar med tillämpningsområdet det kapitlet. För att undvika dubbelreglering inför FI en begränsning i tillämpningsområde för 3 kap. i SRK-föreskrifterna, som innebär att 3 kap. inte ska tillämpas på hantering av IKT-risker som enligt i kapitel II i Dora-förordningen.

Termen ”it-system” tas bort i 5 kap. 4 §, eftersom paragrafen innehåller krav på att ett företag, när det inför nya eller väsentligt förändrade it-system, ska hantera de risker som kan uppstå i samband med detta på ett effektivt och ändamålsenligt sätt. Paragrafen innebär en dubbelreglering i förhållande till artikel 6, 7 och 8.3 Dora-förordningen, som bland annat innehåller krav på att företagen löpande ska hantera IKT-risker och göra en riskbedömning vid varje större förändring av nätverks- och informationssystemets infrastruktur. När det gäller sådana förändringar ska företagen således följa de krav som följer av Dora-förordningen.

Svenska Bankföreningen har ifrågasatt om 5 kap. 4 § innehåller en dubbelreglering i förhållande till de angivna artiklarna, eftersom de artiklarna inte motsvarar bestämmelsen i 5 kap. 4 §. FI anser att det som avgör om en dubbelreglering föreligger eller inte är om bestämmelserna i de två regleringarna rör samma sak, inte om de ser likadana ut. Eftersom det i Dora-förordningen finns bestämmelser om vilka åtgärder ett företag ska vidta i

samband med varje större förändring av nätverks- och informationssystemets infrastruktur, kan föreskrifterna inte innehålla några bestämmelser om detta. Svenska Bankföreningens synpunkt föranleder därför inte någon justering av förslaget.

Bestämmelserna i 5 kap. i SRK-föreskrifterna innehåller krav på företagens riskhantering och innebär i vissa delar en dubbelreglering i förhållande till kapitel II–V i Dora-förordningen när det handlar om IKT-risker. FI inför därför en begränsning i tillämpningsområde för det kapitlet som innebär att kapitlet inte gäller för sådan hantering av IKT-risker som avses i Dora-förordningen.

Svenska Bankföreningen och Sparbankernas Riksförbund har efterlyst ett förtydligande av huruvida IKT-risker enligt Dora-förordningen ingår i begreppet ”alla väsentliga risker” 7 kap. 3 § i föreskrifterna, vilket i så fall skulle innebära att funktionen för riskkontroll ska ansvara för identifiering, hantering och kontroll av dem. Av 7 kap. 3 § framgår vad funktionen för riskkontroll ska utföra för arbete, vilka delar av verksamheten som den ska kontrollera och på vilket sätt. Det är sådant arbete som ska utföras oavsett om de materiella kraven för hur riskerna ska hanteras finns i Dora-förordningen eller i någon annan författning. Hantering av IKT-risker är inte undantagen från det som riskkontrollfunktionen ska kontrollera och övervaka, vilket innebär att de riskerna omfattas av begreppet ”väsentliga risker”.

Begreppet ”it-system” bör inte tas bort i 7 kap. 3 § 9 och i 8 kap. 3 § 5 i SRK-föreskrifterna, vilket Svenska Bankföreningen har ställt frågor om. Bestämmelserna 7 kap. 3 § 9 och i 8 kap. 3 § 5 i föreskrifterna handlar om vilket arbete som funktionerna för riskkontroll (7 kap.) och regelefterlevnad (8 kap.) ska utföra, något som Dora-förordningen inte reglerar. Därför uppkommer ingen dubbelreglering mellan SRK-föreskrifterna och Dora-förordningen i denna del.

I 10 kap. i SRK-föreskrifterna finns bestämmelser om uppdragsavtal. Bland annat finns bestämmelser om att uppdrag ska regleras i skriftliga avtal och om utformningen dessa avtal. I kapitel V i Dora-förordningen finns bestämmelser om hantering risker som kan uppstå i samband med att ett företag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör, inbegripet krav på kontraktsmässiga arrangemang (uppdragsavtal), se artikel 28.4, och på avtalsbestämmelser, se artikel 30. För att undvika dubbelreglering ska 10 kap. inte gälla för sådana uppdragsavtal som regleras i

Dora-förordningen. Däremot ska 10 kap. alltjämt tillämpas på andra uppdragsavtal än de som omfattas av Dora-förordningen.

Eftersom det införs hänvisningar till Dora-förordningen i ett antal bestämmelser i föreskrifterna, ska det även införas en definition av förordningen i dem.

2.3.7 Föreskrifterna om operativa risker

Finansinspektionens ställningstagande: Bestämmelserna i föreskrifterna ska inte gälla för hantering av sådana IKT-risker som avses i Dora-förordningen.

Bestämmelserna om identifiering och mätning (3 kap. 1 §), process för godkännande (5 kap. 10 §) och utseende av person för att hantera risker i samband med nyheter (5 kap. 14 §) ska inte längre gälla för it-system.

Upplysningsbestämmelserna i 5 kap. 8 och 9 §§ ska upphöra att gälla, liksom bestämmelsen om huvudsakligt it-driftställe (5 kap. 19 §).

Därutöver görs redaktionella ändringar.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Svenska Bankföreningen* efterfrågar ett förtydligande om hur bestämmelserna i 5 kap. 1 § ska tolkas i förhållande till Dora-förordningens bestämmelser om finansiella entiteters riskhantering av kritiska eller viktiga funktioner. Vidare framför Svenska Bankföreningen synpunkter på att begreppet ”it-system” har tagits bort och efterfrågar en beskrivning av hur bestämmelserna i föreskrifterna ska tolkas vad gäller krav på riskhantering i samband med större förändringar i förhållande till Dora-förordningen. När det gäller nya 5 kap. 8 §, som handlar om att företagen ska ha en process för att godkänna väsentliga förändringar, delar inte Svenska Bankföreningen bedömningen att motsvarande krav återfinns i artiklarna 6, 7 och 8.3 i Dora-förordningen. Vidare påpekar Svenska Bankföreningen att begreppet ”it-system” finns kvar i nya 5 kap. 9 §, vilket ytterligare försvårar förståelsen av reglerna om processen för godkännande.

Finansinspektionens skäl: Föreskrifterna om operativa risker gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar och vissa värdepappersbolag som också, i egenskap av

kreditinstitut respektive värdepappersföretag, omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 a och e). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

För att anpassa föreskrifterna så att de inte står i strid med Dora-förordningen krävs att sådana bestämmelser i föreskrifterna som har ett innehåll som numera återfinns i Dora-förordningen stryks. Nationella bestämmelser inte får reglera samma sak som Dora-förordningen.

Det är Dora-förordningen som ska gälla för hantering av IKT-risker och föreskrifterna om operativa risker som ska för gälla för hantering övriga risker som omfattas av de föreskrifterna. Det ankommer inte på FI att inom ramen för detta regelärende närmare redogöra för hur Dora-förordningen ska tolkas i olika avseenden, utan endast att förklara varför vissa bestämmelser tas bort eller får ett snävare tillämpningsområde när det i Dora-förordningen finns bestämmelser i samma ämne.

I 1 kap. 2 § införs en begränsning för föreskrifternas tillämpningsområde som innebär att föreskrifterna inte ska tillämpas för att hantera sådana IKT-risker som avses i Dora-förordningen. Begränsningen införs för att undvika dubbelreglering och tydliggöra att hanteringen av IKT-risker ska ske enligt Dora-förordningen. Föreskrifterna om operativa risker ska alltjämt gälla för hantering av andra operativa risker än IKT-risker.

Termen ”it-system” tas bort ur bestämmelsen om riskidentifiering (3 kap. 1 §) samt ur bestämmelser om processen för godkännande (nya 5 kap. 8 och 12 §§). Skälet till att ta bort termen där är att FI vill tydliggöra att de företag som faller inom Dora-förordningens tillämpningsområde ska hantera operativa risker med knytning till it-system enligt Dora-förordningen. Nuvarande 5 kap. 10 § ändras även språkligt.

Svenska Bankföreningen har, när det gäller en bestämmelse om processen för godkännande (nya 5 kap. 8 §), anfört att artiklarna 6, 7 och 8.3 i Dora-förordningen, inte har motsvarande innehåll. Det avgörande för om en dubbelreglering föreligger är dock, som FI redan uttalat, inte om bestämmelserna i de två regleringarna ser likadana ut, utan om de rör samma sak.

Eftersom det i Dora-förordningen finns bestämmelser om vad ett företag ska vidta för åtgärder i samband med varje större förändring av nätverks- och informationssystemets infrastruktur, kan föreskrifterna inte innehålla några

bestämmelser i denna del. Svenska Bankföreningens synpunkt föranleder därför inte någon justering av förslaget.

Inte heller föranleder Svenska Bankföreningens påpekande om begreppet ”it-system” i nya 5 kap. 9 § någon justering av förslaget, eftersom den bestämmelsen endast innehåller en beskrivning av vad de interna reglerna ska innehålla. Bestämmelsen innehåller däremot inte några materiella krav på hantering av IKT-risker, varför den inte utgör någon dubbelreglering i förhållande till Dora-förordningen.

Bestämmelserna i 5 kap. 8 och 9 §§ upphör att gälla. Paragraferna innehåller en upplysning om att bestämmelser om informationssäkerhet finns i 2 kap. i it-föreskrifterna och bestämmelser om hantering av it-system finns i 3 kap. i it-föreskrifterna. Dessa hänvisningar tas bort eftersom 2 och 3 kap. i it-föreskrifterna upphör att gälla (se avsnitt 2.3.8 nedan).

Bestämmelsen i 5 kap. 19 § upphör att gälla. Paragrafen innehåller bland annat krav på att företag ska se till att dess huvudsakliga it-driftsställe finns på ett tillräckligt stort geografiskt avstånd från den plats där företaget förvarar sina säkerhetskopior. Paragrafen innebär en dubbelreglering i förhållande till artikel 12 i Dora-förordningen, som bland annat innehåller bestämmelser om strategier och förfaranden för säkerhetskopiering, och ska därför utgå.

När 5 kap. 19 § upphör att gälla så upphör även det allmänna råd som i dag är knutet till paragrafen att gälla. Mot bakgrund av de ändringar som görs i föreskrifterna får vissa bestämmelser en ny beteckning.

2.3.8 It-föreskrifterna

Finansinspektionens ställningstagande: It-föreskrifterna upphävs och ersätts av nya föreskrifter och allmänna råd om insättningssystem. Bestämmelserna i it-föreskrifterna om informationssäkerhet och it-verksamhet förs inte över till de nya föreskrifterna. Inte heller de bestämmelser om insättningssystem som tar sikte på it-system (4 kap. 3 och 5 §§) förs över till de nya föreskrifterna. Övriga bestämmelser om insättningssystem i it-föreskrifterna förs över till de nya föreskrifterna.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Svenska Bankföreningen* har ställt en fråga om

huruvida FI anser att ett ledningssystem för informationssäkerhet är att likställa med en IKT-riskhanteringsram i enlighet med artikel 6 i Dora-förordningen.

Finansinspektionens skäl: It-föreskrifterna gäller för bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar och värdepappersbolag som avses i 1 kap. 2 § första stycket 7 c – g lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag. Dessa institut omfattas också av Dora-förordningens tillämpningsområde i egenskap av kreditinstitut respektive värdepappersföretag (se artikel 2.1 a och e). It-föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

It-föreskrifterna innehåller krav på informationssäkerhet och it-verksamhet för företag som även omfattas av Dora-förordningen. Genom it-föreskrifterna omvandlades olika riktlinjer från flera internationella institutioner, såsom Europeiska bankmyndigheten, rörande operativa risker och hanteringen av till exempel säkerhetsrisker och informationssäkerhetsarbete, till svenska författningsbestämmelser.

Dora-förordningen innehåller i artiklarna 5–9, 11 och kapitel V bestämmelser om informationssäkerhet och it-verksamhet. Sådana bestämmelser finns även i artiklarna 2, 12, 14 och 21 i kommissionens delegerade förordning (EU) 2024/1774.[7] En dubbelreglering uppstår om inte bestämmelserna i it-föreskrifterna som tar upp de nämnda ämnena upphör att gälla. Av det skälet ska bestämmelserna i 2 kap., 3. kap., och 4 kap. 3 och 5 §§ it-föreskrifterna utmönstras.

När det gäller begreppet ledningssystem, som *Svenska Bankföreningen* efterfrågar ett förtydligande om, konstaterar FI att det i de nu gällande föreskrifterna anges att ett företag ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ett ledningssystem. Hur företagen ska arbeta med informationssäkerhet och vilka krav som ställs regleras också i artikel 6 i Dora-förordningen, som ställer krav på att en finansiell entitet ska ha en IKT-riskhanteringsram.

[7] Kommissionens delegerade förordning (EU) 2024/1774 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar verktyg, metoder, processer och strategier för IKT-riskhantering och den förenklade IKT-riskhanteringsramen

Kravet i de nu gällande it-föreskrifterna på att ett företaget ska använda ett ledningssystem överensstämmer i så hög grad med kravet på IKT-hanteringsram i Dora-förordningen att dessa båda krav inte bör gälla samtidigt för ett företag. Detta är skälet till att kravet på ett ledningssystem i 2 kap. i it-föreskrifterna tas bort. Detta betyder dock inte att innebörden av begreppet ledningssystem i it-föreskrifterna är densamma som innebörden av begreppet IKT-hanteringsram enligt Dora-förordningen. FI kan inte därutöver göra uttalanden om tolkningen av begreppet IKT-hanteringsram i detta regelärende.

Eftersom förändringarna i sak i it-föreskrifterna innebär att huvuddelen av bestämmelserna i dem tas bort, upphävs it-föreskrifterna och ersätts av nya föreskrifter och allmänna råd om insättningssystem. De bestämmelser i it-föreskrifterna som inte ska tas bort förs över till de nya föreskrifterna och allmänna råden.

2.3.9 Rapporteringsföreskrifterna för försäkringsrörelse

Finansinspektionens ställningstagande: Bestämmelserna i rapporteringsföreskrifterna för försäkringsrörelse om rapportering av väsentliga händelser ska inte gälla för rapportering av sådana allvarliga IKT-relaterade incidenter som avses i artikel 19 i Dora-förordningen.

Remisspromemorian: Innehöll inte något förslag i denna del.

Remissinstanserna: De flesta remissinstanserna lämnar inga synpunkter i denna del. *Svensk Försäkring* efterfrågar ändringar i rapporteringsföreskrifterna för försäkringsrörelse av den innebörden att rapportering av allvarliga IKT-relaterade incidenter enligt artikel 19 Dora-förordningen undantas från föreskrifternas tillämpningsområde, i syfte att undvika dubbla krav på rapportering.

Finansinspektionens skäl: I 4 kap. i rapporteringsföreskrifterna för försäkringsrörelse finns bland annat bestämmelser om att försäkringsföretag ska rapportera när vissa händelser inträffar i verksamheten. Det handlar bland annat om händelser som kan äventyra företagets stabilitet eller dess förmåga att uppfylla sina åtaganden mot försäkringstagare och andra ersättningsberättigade.

Genom Dora-förordningen införs krav på IKT-relaterad incidentrapportering (Kapitel III i Dora-förordningen). För att undvika dubbla krav på rapportering beslutar FI, i enlighet med den remissynpunkt som har lämnats

av *Svensk Försäkring*, att bestämmelserna i 4 kap. rapporteringsföreskrifterna för försäkringsrörelse inte ska gälla för rapportering av sådana allvarliga IKT-relaterade incidenter som avses i artikel 19 i Dora-förordningen. En bestämmelse om detta införs i de föreskrifterna.

2.3.10 Föreskrifterna om betaltjänstverksamhet

Finansinspektionens ställningstagande: Kravet på att ta fram säkerhetsåtgärder som hanterar konfidentialitet, integritet och tillgänglighet för data och it-system tas bort i de bestämmelser som handlar om det system för hantering av operativa risker och säkerhetsrisker som en betaltjänstleverantör ska ha (5 kap. 1 § 7). Bestämmelserna om systemet för hantering av operativa risker och säkerhetsrisker ska inte gälla för att hantera sådana IKT-risker som omfattas av Dora-förordningen.

Bestämmelserna om att en betaltjänstleverantör ska rapportera en allvarlig operativ incident eller säkerhetsincident till FI samt informera sina betaltjänstanvändare om händelsen (6 kap. 4 och 5 §§), ska upphöra att gälla.

Därutöver görs vissa redaktionella ändringar.

Remisspromemorian: Förslaget hade i sak samma innehåll, dock har vissa redaktionella ändringar tillkommit i förhållande till det remitterade förslaget.

Remissinstanserna: De remissinstanser som har yttrat sig har inte haft några synpunkter på förslaget.

Finansinspektionens skäl: Föreskrifterna om betaltjänstverksamhet gäller för kreditinstitut, betalningsinstitut, registrerade betaltjänstleverantörer, institut för elektroniska pengar och registrerade utgivare av elektroniska pengar, vilka alla också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 a, b och d). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

I 5 kap. 1 § första stycket finns bestämmelser som innehåller krav på en betaltjänstleverantörs system för operativa risker och säkerhetsrisker. Enligt 5 kap. 1 § första stycket 7 ska betaltjänstleverantören ta fram säkerhetsåtgärder som hanterar konfidentialitet, integritet och tillgänglighet för data och it-system, samt fysisk säkerhet och åtkomstkontroll.

Kravet på att ta fram säkerhetsåtgärder som hanterar konfidentialitet, integritet och tillgänglighet för data samt it-system tas bort, eftersom det annars skulle utgöra en dubbelreglering i förhållande till artikel 7 och 9 i Dora-förordningen. Dessa artiklar innehåller krav på att IKT-system ska vara uppdaterade, tillförlitliga, tekniskt motståndskraftiga och håller hög standard för tillgänglighet, äkthet, integritet och konfidentialitet avseende data.

Vidare införs ett nytt andra stycke i den bestämmelse – 5 kap. 1 § – som handlar om det system för hantering av operativa risker och säkerhetsrisker som en betaltjänstleverantör ska ha. I det stycket bör det anges att första stycket inte gäller för sådana IKT-risker som omfattas av Dora-förordningen. Skälet för att införa ett andra stycket är att bestämmelsen, utöver de krav som tas bort i punkten 7, även innehåller allmänna krav på operativa risker och säkerhetsrisker. Detta innebär en dubbelreglering i förhållande till Dora-förordningen till den del som bestämmelsen avser IKT-risker. Genom bestämmelsen i det nya andra stycket undviks sådan dubbelreglering.

Enligt 6 kap. 4 § ska en betaltjänstleverantör rapportera allvarliga operativa incidenter eller säkerhetsincidenter som uppkommit i verksamheten till FI. Vidare ska en betaltjänstleverantör informera sina betaltjänstanvändare om det inträffat en allvarlig operativ incident eller säkerhetsincident som kan påverka deras ekonomiska intressen negativt (6 kap. 5 §). FI beslutar att bestämmelserna ska upphöra att gälla eftersom sådan rapporteringsplikt och informationsplikt som finns i bestämmelserna följer av artikel 19 i Dora-förordningen. Behovet av rapporteringskravet och informationskravet i föreskrifterna bortfaller därför i och med att Dora-förordningen börjar tillämpas.

2.3.11 Pensionsstiftelseföreskrifterna

Finansinspektionens ställningstagande: Finansinspektionens föreskrifter (FFFS 2019:19) om pensionsstiftelser ska inte ändras till följd av Dora-förordningen.

Remisspromemorian: Remisspromemorian behandlade inte frågan.

Remissinstanserna: De flesta remissinstanserna lämnar inga synpunkter i denna del. *Svenska Pensionsstiftelsers Förening (SPFA)* noterar att det inte föreslås några ändringar i Finansinspektionens föreskrifter (FFFS 2019:19) om pensionsstiftelser, nedan pensionsstiftelseföreskrifterna. SPFA efterlyser en förklaring till det, samt även en förklaring till varför det inte föreslås några ändringar eller förtydliganden vad gäller till exempel bestämmelserna

i pensionsstiftelseföreskrifterna om riktlinjer för riskhantering, riktlinjer för verksamhet som omfattas av uppdragsavtal och beredskapsplan (3 kap. 1, 4 och 5 §§). SPFA undrar hur dessa bestämmelser förhåller sig till Dora-förordningen.

Finansinspektionens skäl*:* Pensionsstiftelseföreskrifterna gäller i huvudsak för pensionsstiftelser som tryggar utfästelser om pension åt minst 100 personer (se 1 kap. 1 § andra stycket i pensionsstiftelseföreskrifterna och 9 a § andra och tredje styckena lagen [1967:531] om tryggande av pensionsutfästelse m.m., tryggandelagen). Sådana pensionsstiftelser omfattas av Dora-förordningens tillämpningsområde i egenskap av tjänstepensionsinstitut (se artikel 2.1 p). Det behöver därför säkerställas att pensionsstiftelseföreskrifterna inte står i strid med Dora-förordningen.

De bestämmelser som finns i 3 kap. i pensionsstiftelseföreskrifterna gäller innehållet i styrdokument för bland annat riskhantering, uppdragsavtal och beredskapsplan. I 16 § tryggandelagen finns bestämmelser om bland annat en pensionsstiftelses egen riskbedömning och om vilka uppdragsavtal som en stiftelse får ingå. I Dora-förordningens kapitel II och V finns bestämmelser om bland annat finansiella instituts riskbedömning och riskhantering av IKT-risker och IKT-tredjepartsrisker inklusive uppdragsavtal om IKT-tjänster.

Finansinspektionen bedömer att bestämmelserna i 3 kap. pensionsstiftelseföreskrifterna varken står i strid med Dora-förordningen eller innebär en dubbelreglering i förhållande till Dora-förordningen, en fråga som *SPFA* vill se belyst. Skälet för den bedömningen är att pensionsstiftelseföreskrifterna, till skillnad från Dora-förordningen, inte innehåller några materiella krav vad gäller riskhantering, uppdragsavtal och beredskapsplan, utan endast reglerar vad en pensionsstiftelses olika styrdokument ska innehålla. Dora-förordningen, å sin sida, innehåller inte några sådana bestämmelser om innehållet i styrdokument som finns i pensionsstiftelseföreskrifterna

Det krävs därför inte någon ändring i pensionsstiftelseföreskrifterna inom ramen för detta regelärende.

2.3.12 Tjänstepensionsföreskrifterna

Finansinspektionens ställningstagande: Bestämmelserna om uppdragsavtal ska inte gälla för sådana uppdragsavtal som omfattas av kapitel V i Dora-förordningen.

Remisspromemorian: Innehöll i huvudsak samma förslag. I förslaget placerades den nya undantagsbestämmelsen i ett nytt stycke i en befintlig paragraf i stället för i en ny paragraf.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Svensk Försäkring* anför att den föreslagna ändringen avseende uppdragsavtal bör placeras i en egen paragraf i stället för ett nytt stycke i 8 kap. 2 §, eftersom den paragrafen endast gäller för mindre tjänstepensionsföretag. *Tjänstepensionsförbundet* vill se ett förtydligande om huruvida uppdragsavtal om IKT-tjänster, med hänsyn till artikel 28.3 Dora-förordningen, även fortsättningsvis ska anmälas enligt 9 kap. 25 § lagen (2019:742) om tjänstepensionsföretag, samt om det sätt på vilket uppdragsavtal som rör kritiska eller viktiga funktioner ska anmälas.

Finansinspektionens skäl: Tjänstepensionsföreskrifterna gäller för tjänstepensionsföretag som också i egenskap av tjänstepensionsinstitut omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 p). De föreskrifterna behöver därför anpassas så att de inte står i strid med Dora-förordningen.

I 8 kap. i tjänstepensionsföreskrifterna finns bestämmelser om uppdragsavtal. I kapitel V i Dora-förordningen finns bestämmelser om hantering av risker som kan uppstå i samband med att ett företag använder IKT-tjänster som tillhandahålls av en tredjepartsleverantör. De bestämmelserna innehåller krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering införs det i föreskrifterna en bestämmelse om att 8 kap. 69, 70 och 71 §§ inte ska gälla för sådana uppdragsavtal som regleras i Dora-förordningen. FI delar Svensk Försäkrings bedömning att denna bestämmelse bör placeras i en egen paragraf. FI beslutar därför att en ny paragraf, 8 kap. 2 a §, ska införas.

Bestämmelserna i tjänstepensionsföreskrifterna om uppdragsavtal ska alltjämt gälla för andra uppdragsavtal än sådana som avses i Dora-förordningen. När det gäller den anmälningsskyldighet som följer av 9 kap. 25 § lagen (2019:742) om tjänstepensionsföretag och hur den förhåller sig till kraven i artikel 28.3 om anmälan av uppdragsavtal, en fråga som *Tjänstepensionsförbundet* tar upp, kan FI inte påverka innehållet i vare sig lagen om tjänstepensionsföretag eller Dora-förordningen. FI kan därför inte inom detta regelärende lämna några sådana förtydliganden som Tjänstepensionsförbundet efterlyser.

2.3.13 Rapporteringsföreskrifterna för tjänstepensionsföretag

Finansinspektionens ställningstagande: Bestämmelserna om incidentrapportering i rapporteringsföreskrifterna för tjänstepensionsföretag ska inte gälla för uppgifter om sådana allvarliga IKT-relaterade incidenter som avses i Dora-förordningen.

Remisspromemorian: Innehöll inte något förslag i denna del.

Remissinstanserna: De flesta remissinstanserna framför inga synpunkter i denna del. *Svensk Försäkring* och *Tjänstepensionsförbundet* efterfrågar en ändring i rapporteringsföreskrifterna för tjänstepensionsföretag som undantar rapportering av allvarliga IKT-relaterade incidenter enligt artikel 19 i Dora-förordningen från rapporteringsföreskrifterna, så att dubbelrapportering kan undvikas.

Finansinspektionens skäl: I 3 kap. i rapporteringsföreskrifterna för tjänstepensionsföretag finns bland annat bestämmelser om att ett tjänstepensionsföretag ska rapportera när vissa händelser inträffar i verksamheten. Det handlar bland annat om händelser som kan äventyra företagets stabilitet eller dess förmåga att uppfylla sina åtaganden, exempelvis på grund av att fel uppstår i tekniska system. Genom Dora-förordningen införs krav på IKT-relaterad incidentrapportering (Kapitel III i Dora-förordningen).

FI delar *Svensk Försäkrings* och *Tjänstepensionsförbundets* uppfattning att det bör införas en undantagsbestämmelse i rapporteringsföreskrifterna för tjänstepensionsföretag för att det inte ska ställas dubbla krav på rapportering av uppgifter om sådana händelser som både omfattas av 3 kap. i föreskrifterna och artikel 19 i Dora-förordningen. FI beslutar därför att sådana allvarliga IKT-relaterade incidenter som omfattas av artikel 19 Dora-förordningen ska undantas från tillämpningsområdet för 3 kap. i rapporteringsföreskrifterna för tjänstepensionsföretag.

2.3.14 Clearingföreskrifterna

Finansinspektionens ställningstagande*:* Det införs nya paragrafer i 3 kap. clearingföreskrifterna som motsvarar 5 kap. 4 § SRK-föreskrifterna och 5 kap. 10–14 §§ föreskrifterna om operativa risker. Hänvisningarna i clearingföreskrifterna till de bestämmelserna tas bort.

Vissa redaktionella ändringar görs i clearingföreskrifterna.

Remisspromemorian: Förslaget hade samma innehåll.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Riksbanken* menar att det är viktigt att clearingbolag uppfyller samma krav som Dora-förordningen ställer på andra finansiella företag, men noterar att föreskrifterna inte har uppdaterats i det hänseendet.

Finansinspektionens skäl*:* Clearingbolag omfattas inte av Dora-förordningens tillämpningsområde. Dessa bolag bör alltså även i fortsättningen omfattas av en reglering i FI:s föreskrifter om it-system.

När det gäller styrning och riskhantering finns i clearingföreskrifterna relativt omfattande hänvisningar till SRK-föreskrifterna och föreskrifterna om operativa risker. Eftersom de föreskrifterna nu ändras (se avsnitt 2.3.6 och 2.3.7), uppstår ett behov av ändringar även i clearingföreskrifterna.

Eftersom kraven på riskhantering och en process för godkännande i 5 kap. 4 § SRK-föreskrifterna och 5 kap. 10–14 §§ föreskrifterna om operativa risker ändras så att bestämmelserna inte längre omfattar it-system, införs nya bestämmelser i clearingföreskrifterna som motsvarar den nuvarande lydelsen av de bestämmelserna. Detta krävs eftersom föreskriftskraven på clearingbolagen annars faller bort till den del de avser it-system. Vissa språkliga justeringar görs i bestämmelserna i samband med att de förs över till clearingföreskrifterna.

Av den nuvarande lydelsen av 5 kap. 10 och 11 §§ föreskrifterna om operativa risker framgår att ett företag vid tillämpningen av bestämmelserna ska ta hänsyn till verksamhetens art, omfattning och komplexitet. Detta följer emellertid redan av 1 kap. 4 § i clearingföreskrifterna, varför det saknas skäl att i clearingföreskrifterna införa bestämmelser som motsvarar 5 kap. 10 § andra stycket och 5 kap. 11 § andra stycket i föreskrifterna om operativa risker.

Till följd av den omnumrering som görs i SRK-föreskrifterna samt att vissa nya bestämmelser förs in i clearingföreskrifterna, görs även justeringar i 3 kap. 1 § i clearingföreskrifterna så att hänvisningarna där blir korrekta. De nya bestämmelserna om process för godkännande placeras i direkt anslutning till bestämmelserna om riskhantering.

När det gäller *Riksbanken*s synpunkt att även clearingbolagen bör uppfylla samma krav som Dora-förordningen ställer på andra finansiella institut, så konstaterar FI att regering och riksdag inte har valt att ställa sådana krav på clearingbolagen. Det ankommer inte på FI att utsträcka Dora-förordningens tillämpningsområde längre än vad lagstiftaren har valt att göra.

2.4 Ikraftträdande- och övergångsbestämmelser

Finansinspektionens ställningstagande: De nya och ändrade föreskrifterna och allmänna råden ska träda i kraft den 17 januari 2025. Rapportering av informationsregister ska göras första gången senast den 15 april 2025. Den version av registret som då ska lämnas in till FI ska avse förhållandena vid utgången av mars 2025.

Remisspromemorian: Förslaget hade samma innehåll när det gäller tidpunkten för ikraftträdande. I remisspromemorian föreslogs att rapporteringen av informationsregister enligt artikel 28.3 i Dora-förordningen skulle lämnas första gången senast den 28 februari 2025 och avse förhållandena vid utgången av januari 2025.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Svenska Bankföreningen*, *Svensk Försäkring* och *Svenska Försäkringsförmedlares Förening* föreslår en framflyttning av den första rapporteringen av informationsregistret eftersom det saknas detaljer kring format för rapportering och det dessutom kan förväntas tydligare riktlinjer från de europeiska tillsynsmyndigheterna framöver. Även *Tjänstepensionsförbundet, Fondbolagens Förening* och *Sparbankernas Riksförbund* anser att de föreslagna tidpunkterna ligger för nära i tiden, mot bakgrund av att de tekniska standarderna om rapporteringen ännu inte har antagits av Europeiska kommissionen. Även *Finansbolagens Förening* anför att tiden som återstår till det första rapporteringstillfället är för kort.

Tilläggsremissen: Förslaget hade samma innehåll när det gäller tidpunkten för den första rapporteringen av informationsregister och vad den rapporteringen ska avse. Inget annat förslag lämnades i fråga om tidpunkten för ikraftträdande.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *SFBF* och *Tjänstepensionsförbundet* påpekar att även om det är bra att tidpunkten senareläggs, så är det av största vikt att de tekniska förutsättningarna för inrapporteringen tydliggörs så snart som möj-

ligt, eftersom det är en förutsättning för att rapporteringen ska kunna göras överhuvudtaget. *SPFA* ifrågasätter om tiden är tillräcklig, eftersom den tekniska lösningen för inrapporteringen inte är färdig. *Svenska Bankföreningen*, med vilken *Svensk Försäkring* instämmer, avstyrker förslaget att rapporteringen 2025 ska göras senast den 15 april. Som skäl anför Svenska Bankföreningen dels att det inte är lämpligt att beslut om datum fattas innan den tekniska standard som ska gälla för inrapporteringen har beslutats, dels att den förkortade tid som förslaget innebär mellan den tidpunkt som rapporteringen ska avse till dess att rapporteringen ska lämnas in innebär en ökad risk för fel. Det måste särskilt beaktas att det är första gången som registret ska skickas in och att företagen har att beakta eventuella ändringar som görs i de tekniska standarderna innan de beslutas. Även *Finansbolagens Förening* anför att det inte är rimligt att finansiella entiteter får kortare tid att genomföra den första rapporteringen, jämfört med senare rapporteringar. Vidare anser Svenska Bankföreningen att tidpunkten för den första inrapporteringen av informationsregistret ska infalla tidigast sex månader efter det att den tekniska standarden är godkänd och att tiden för att förbereda informationsregistret inför inrapporteringen ska bestämmas till minst 30 dagar. Svenska Bankföreningen anser även att de föreslagna datumen ska vara desamma inom hela EU. *Swedish Financial Technology Association (SweFinTech)* anser inte heller att det är lämpligt att sätta ett datum innan den tekniska standarden om informationsregistret är klar och anför att tidpunkten för den första rapporteringen bör bestämmas till minst tre månader efter det att den tekniska standarden har antagits. Även *Svensk Försäkring* har anfört att FI bör avvakta med ett beslut om tidpunkt för den första rapporteringen av informationsregistret till dess att alla tekniska och praktiska förutsättningar för rapporteringen är fastställda och kommunicerade. Även *Sparbankernas Riksförbund* har anfört att rapporteringspliktiga företag måste ges rimlig tid att planera, populera och validera sina register efter det att förutsättningarna för registret är beslutade, och att FI:s val av tidpunkt i större utsträckning behöver ta hänsyn till det. Vidare anför Sparbankernas Riksförbund att FI bör verka för att de europeiska tillsynsmyndigheterna omprövar sitt beslut om rapporteringsplikt för de behöriga myndigheterna.

Finansinspektionens skäl: De nya och ändrade föreskrifterna och allmänna råden hänger mycket nära samman med Dora-förordningen och den kompletterande nationella reglering som införs på lag- och förordningsnivå. FI:s nya reglering ska därför träda i kraft vid samma tidpunkt som Dora-förord-

ningen börjar gälla i medlemsstaterna och den kompletterande svenska regleringen träder i kraft, dvs. den 17 januari 2025.

Som framgår ovan i avsnitt 2.1 fattade de europeiska tillsynsmyndigheterna den 8 november 2024 beslut om tidpunkterna för de behöriga myndigheternas årliga rapportering av informationsregister till de europeiska tillsynsmyndigheterna. Beslutet är bindande för de behöriga myndigheterna, däribland FI. I beslutet anges att de behöriga myndigheterna ska vidarebefordra de första informationsregistren som företagen har lämnat in senast den 30 april 2025. Av avsnitt 2.1 framgår också att Europeiska kommissionen den 29 november 2024 fattade beslut om en genomförandeförordning (en så kallad teknisk standard för genomförande) som fastställer de mallar som ska användas för rapportering av informationsregister enligt artikel 28.3 i Dora-förordningen.

Eftersom datum för de behöriga myndigheternas vidarerapportering redan är beslutat av de europeiska tillsynsmyndigheterna, och mallarna för rapporteringen av informationsregister har beslutats av Europeiska kommissionen, saknas det utrymme för FI att, som *Svenska Bankföreningen*, *Svensk Försäkring* och *SweFinTech* efterfrågar, avvakta med att fatta beslut om när företagen första gången ska lämna in registret till FI. Detta gäller även om FI skulle verka för att de europeiska tillsynsmyndigheterna omprövar sitt beslut, som *Sparbankernas Riksförbund* förordat. FI behöver nu se till att rapporteringen till de europeiska tillsynsmyndigheterna lämnas i tid.

Svenska Bankföreningen, Svensk Försäkring, *Svenska Försäkringsförmedlares Förening*, *Tjänstepensionsförbundet*, *Fondbolagens Förening*, *SFBF, SPFA,* Sparbankernas Riksförbund, och *Finansbolagens Förening* framför synpunkter om att det tekniska formatet för rapporteringen av informationsregister ännu inte har beslutats på europeisk nivå och att tiden som återstår till den första rapporteringen är för snäv. FI konstaterar att arbetet i denna del inte är slutfört på europeisk nivå. FI kommer dock att publicera information om det tekniska formatet för rapporteringen så fort de europeiska tillsynsmyndigheterna har tagit ställning i den frågan. Att de mallar som ska användas vid rapporteringen nu har beslutats av Europeiska kommissionen i form av en genomförandeförordning torde i viss mån kunna underlätta för företagen att påbörja arbetet med informationsregistret.

Tidsutrymmet från den tidpunkt som den första rapporteringen av informationsregister ska avse till den tidpunkt då rapporteringen ska lämnas är kortare enligt förslaget i tilläggsremissen (utgången av mars 2025 respektive

den 15 april 2025) än enligt förslaget i remisspromemorian (utgången av januari 2025 respektive den 28 februari 2025). Denna förkortning, en fråga som tas upp av Finansbolagens Förening, Sparbankernas Riksförbund och Svenska Bankföreningen, är helt föranledd av det beslut som de europeiska tillsynsmyndigheterna har fattat. Förslaget i tilläggsremissen innebär å andra sidan att företagen får mer tid på sig än enligt förslaget i remisspromemorian från de nya föreskrifternas ikraftträdande till dess att den första rapporteringen ska lämnas, något som ett flertal remissinstanser efterlyser, bland annat Svenska Bankföreningen, Svensk Försäkring och Tjänstepensionsförbundet.

Finansinspektionen finner sammantaget, trots vad flera remissinstanser anför om den tid som står till förfogande för förberedelser inför det första rapporteringstillfället och för sammanställningen av den version av informationsregistret som ska lämnas då, att de finansiella entiteterna som står under FI:s tillsyn ska lämna den första rapporteringen av informationsregister enligt artikel 28.3 i Dora-förordningen senast den 15 april 2025 och att den version av informationsregistret som då ska lämnas in ska avse förhållandena vid utgången av mars 2025. Den första rapporteringen kan inte ske senare än så om FI ska hinna vidarerapportera enligt de europeiska tillsynsmyndigheternas beslut, senast den 30 april 2025.

Även om datum för företagens inlämning av sina register till den nationella tillsynsmyndigheten kan variera mellan olika medlemsstater i EU, som *Svenska Bankföreningen* påpekar, torde varierationerna vara små, eftersom de behöriga myndigheterna i alla medlemsstater behöver vidarerapportera till de europeiska tillsynsmyndigheterna senast 30 april 2025.

3 Konsekvenser

3.1 Inledning

De nya och ändrade föreskrifterna och allmänna råden som FI beslutar om är en följd av Dora-förordningen. Företagen som anges nedan i punkterna a–s är sådana företag som omfattas av Dora-förordningen och som berörs av de nya föreskrifterna. Företag som är undantagna från förordningens tillämpningsområde enligt artikel 2.3 i Dora-förordningen omfattas inte av de nya föreskrifterna.

a) Kreditinstitut

b) Betalningsinstitut
c) Leverantörer av kontoinformationstjänster
d) Institut för elektroniska pengar
e) Värdepappersbolag
f) Leverantörer av kryptotillgångstjänster
g) Värdepapperscentraler
h) Centrala motparter
i) Handelsplatser
j) Transaktionsregister
k) Förvaltare av alternativa investeringsfonder
l) Fondbolag
m) Leverantörer av datarapporteringstjänster
n) Försäkrings- och återförsäkringsföretag
o) Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet
p) Tjänstepensionsinstitut
q) Administratörer av kritiska referensvärden
r) Leverantörer av gräsrotsfinansieringstjänster
s) Svenska Skeppshypotekskassan.

Regelrådet bedömer att konsekvensutredningen i remisspromemorian uppfyller kraven i förordningen (2024:183) om konsekvensutredningar. Regelrådet påtalar dock att det finns brister i de delar av konsekvensutredningen som handlar om förslagets påverkan på konkurrensen samt om vilka åtgärder som har vidtagits för att begränsa förslagets kostnader och andra effekter.

SPFA efterfrågar en tydligare redogörelse för de överväganden som gjorts om den ökade administrativa och regulatoriska bördan samt riskerna som förslaget kan medföra för de finansiella entiteterna, särskilt mindre aktörer såsom pensionsstiftelser.

Sparbankernas riksförbund anser att det är olyckligt att proportionaliteten inte har beaktats mer eftersom den är ett prioriterat område och då ett uttryckligt uppdrag har lämnats till flera myndigheter att faktiskt minska regelbördan för företagen.

FI har med anledning av de inkomna remissynpunkterna gjort vissa förtydliganden nedan.

Sammantaget uppgår antalet företag som berörs av nya föreskrifter till cirka 1300[8]. Dora-förordningen innehåller proportionalitetsbestämmelser när det gäller de krav på IKT-riskhanteringsramar som berörda företag ska uppfylla till följd av förordningen. Detta innebär att små företag i den delen får vissa lättnader. Det som anges i artikel 28.10 i Dora-förordningen om proportionalitet gäller de tekniska standarder som beslutas av Europeiska kommissionen.

När det gäller krav på tekniskt format för företagens inrapportering saknas det förutsättningar i Dora-förordningen för att ta särskild hänsyn till förutsättningarna för små företag. Genom de föreskriftsändringar som nu beslutas och som syftat till att undvika dubbelreglering, gör FI bedömningen att den administrativa och regulatoriska bördan har minskat något för berörda företag, jämfört med om några sådana ändringar inte hade gjorts.

I avsnitten 1.1 och 1.3 finns en beskrivning av vad FI vill uppnå med de föreslagna ändringarna i berörda föreskrifter och vilka regleringsalternativ som finns. För uppgifter om de bemyndiganden som ligger till grund för förslaget, se avsnitt 1.4.

FI bedömer att föreskrifterna överensstämmer med och inte går utöver Sveriges skyldigheter som medlemsstat i EU.

FI redogör nedan för de konsekvenser som de nya föreskrifterna bedöms få för samhället och konsumenterna, företagen samt FI. FI bedömer inte att regleringen får några effekter av betydelse för företagens förutsättningar för arbete eller villkor i övrigt.

När det gäller påverkan på konkurrensen, en fråga som *Regelrådet* önskat se en ytterligare behandling av, gör FI följande bedömning.

Av artikel 4 i Dora-förordningen följer att företagen ska genomföra reglerna om IKT-riskhanteringsramen i enlighet med proportionalitetsprincipen, det vill säga med beaktande av sin storlek och allmänna riskprofil, omfattningen och komplexiteten av sina tjänster samt verksamhet och insatser. Detta gynnar särskilt små företag. Det kan inte uteslutas att de lättnader som Dora-förordningen innehåller för mindre företag avseende IKT-riskhanteringsramen i viss utsträckning kan påverka konkurrensen mellan företagen. FI anser dock att det främst handlar om att införa vissa lättnader för mindre

[8] Antalet berörda företag är en uppskattning utifrån det tillämpningsområde som följer av artikel 2 i Dora-förordningen.

företag eftersom kraven annars skulle kunna bli oproportionerligt stränga för dem. Detta kan inte anses påverka konkurrensen negativt.

De nya och ändrade föreskrifterna träder i kraft samtidigt som Dora-förordningen. FI bedömer inte att det är möjligt att ta någon särskild hänsyn vid fastställandet av tidpunkten för ikraftträdande. När det gäller tekniskt format för inrapportering bedömer FI att det finns behov av särskilda informationsinsatser till berörda företag.

FI bedömer att konsekvenserna i huvudsak kommer kunna utvärderas inom ramen för den löpande tillsynen samt efter det att FI erhållit den årliga uppdateringen av företagens informationsregister, dvs. tidigast under 2026.

3.2 Konsekvenser för samhället och konsumenterna

Varken de nya eller ändrade föreskrifterna bedöms påverka konkurrensen mellan företagen på marknaden (se avsnitt 3.1 ovan) eller medföra några konsekvenser för konsumenterna.

3.3 Konsekvenser för företagen

FI redogör nedan för de konsekvenser som de nya och ändrade föreskrifterna innebär för företagen och vilka kostnader som FI uppskattar att föreskrifterna får för företagen.

3.3.1 Tekniskt format för inrapportering enligt de föreslagna nya föreskrifterna

Av Dora-förordningen framgår att företagen ska rapportera allvarliga incidenter till den behöriga myndigheten och upprätta ett informationsregister över vilka avtal om IKT-tjänster som företagen har med tredjepartsleverantörer, samt i vissa fall lämna information till behöriga myndigheter. FI föreslår i föreskrifterna att den inrapportering som ska göras till FI, såväl när det gäller incidentrapportering som informationsregister, ska ske på det sätt som anvisas på FI:s webbplats. Rapporteringen behöver göras i ett format som kan användas både för analys och för vidarerapportering till de europeiska tillsynsmyndigheterna. De finansiella företagens rapportering av både informationsregister respektive incidenter att formatet behöver därför anpassas till de krav som ställs på FI i informationsöverföringen till de europeiska tillsynsmyndigheterna.

Det tekniska format som rapporteringarna ska göras i, kommer att vara av sådant slag som företagen redan har tillgång till genom sedvanlig mjukvara respektive rapportering via FI:s webbplats. Att formatet anpassas på detta sätt bidrar till att hålla nere kostnaderna, jämfört med om rapporteringen skulle göras på ett helt nytt sätt.

FI kommer att tillhandahålla ett gränssnitt för den inrapportering som ska göras. Företagens kostnad i det avseendet blir att säkerställa att de har ett sådant gränssnitt som krävs för att kunna överföra informationen till FI. Den anpassning av it-system som kan behöva göras av företagen är en engångskostnad. Kostnaden varierar från företag till företag beroende på vilken it-lösning företaget har och om arbetet utförs av egen personal eller av konsulter.

FI uppskattar tidsåtgången för arbetet till 40–80 timmar och kostnaden till 60 000–160 000 kronor per företag[9], i form av en engångskostnad.

3.3.2 Datum för inrapportering enligt de föreslagna nya föreskrifterna

Det följer av artikel 28 i Dora-förordningen att företagen, som en del av sin IKT-riskhanteringsram, ska upprätthålla och uppdatera register med information om vilka IKT-tjänster som tillhandahålls av tredjepartsleverantörer. I föreskrifterna anges vilket datum som uppgifterna ska lämnas till FI och vilket referensdatum som de ska ha. Företagen kan i det avseendet behöva göra vissa uppdateringar i sina rapporteringsrutiner, vilket är en engångskostnad. FI bedömer att det rör sig om en begränsad arbetsinsats, uppskattningsvis 10–20 timmar, för att se över och uppdatera sina rapporteringsrutiner. Det innebär en engångskostnad som beräknas uppgå till cirka 15 000 – 30 000 kronor per företag.

Därutöver behöver företagen senast den 28 februari varje år säkerställa att uppgifterna förs över till FI i en samlad rapport och att lämnade uppgifter är riktiga per utgången av föregående kalenderår (med undantag för första rapporteringstillfället, då informationsregistret ska lämnas senast den 15 april 2025 och med referenstidpunkt 31 mars 2025). Detta medför en årlig kostnad för att granska och skicka in uppgifterna till FI, som i sin tur ska vidarebefordra informationen till de europeiska tillsynsmyndigheterna. FI uppskattar att företagens kostnader för att varje år skicka in uppgifterna till

[9] Vid beräkning av kostnaden utgår FI från 2 § förordningen (2009:1237) om timkostnadsnorm inom rättshjälpsområdet. Timkostnadsnormen anges till 1531 kr per timme för 2024.

FI uppgår till uppskattningsvis 10–20 timmar. Detta innebär en årlig kostnad på cirka 15 000–30 000 kronor per företag. I denna beräkning ingår inte kostnader för att initialt upprätta och därefter uppdatera informationsregistret, eftersom det är krav som följer av Dora-förordningen.

3.3.3 Konsekvenser av föreslagna ändringar i befintliga föreskrifter

Ändringarna i befintliga föreskrifter bedöms få begränsade konsekvenser för företagen. Att bestämmelser i föreskrifterna tas bort, att det införs en begränsning för företagen att tillämpa befintliga föreskrifter eller att hänvisningar ändras, bedöms inte få några konsekvenser för företagen. Detta eftersom de berörda företagen inte behöver vidta någon åtgärd till följd av dessa ändringar. Däremot behöver företagen anpassa sin verksamhet till kraven i Dora-förordningen. Konsekvenserna för de berörda företagen av bestämmelserna i Dora-förordningen behandlas dock inte i denna konsekvensanalys.

I de fall som ändringarna innebär att företagens verksamhetsplan ska innehålla viss angiven information, behöver företagen se över om det behövs göra nödvändiga uppdateringar. FI uppskattar att det rör sig om en begränsad arbetsinsats om cirka 5–10 timmar och en engångskostnad på mellan 7 500 och 15 000 kronor.

När det gäller ändringen av 1 a kap. 28 § marknadsplatsföreskrifterna avser den bestämmelsen endast företag som ansöker om tillstånd att bedriva börsverksamhet. Kravet på redogörelsen som avser transparens före handel i verksamhetsplanen, det vill säga hur företaget avser att följa reglerna i Mifir, bedöms endast i marginell utsträckning påverka företag som ansöker om nytt tillstånd.

3.4 Konsekvenser för Finansinspektionen

Föreskrifterna om tekniskt format för inrapportering innebär kostnader för FI genom nedlagd arbetstid för att ta fram it-system som kan hantera mottagande och analys av inrapporterade informationsregister samt IKT-incidentrapporteringarna. FI kommer även ha kostnader för sådan it-hårdvara och programvara som krävs, tillsammans med löpande kostnader för underhåll.