Remisspromemoria

Datum 2024-09-04 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) föreslår 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 föreslås ändringar i olika föreskrifter som gäller för olika delar av finanssektorn.

FI föreslår även nya föreskrifter om i vilket tekniskt format som företagen ska rapportera uppgifter till FI, samt vid vilken tidpunkt som de ska rapportera in informationsregister enligt Dora-förordningen.

De nya och ändrade föreskrifterna och allmänna råden föreslås träda 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

Dora-förordningen[2] 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[3] 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 EU-kommissionen. Samtidigt som Dora-förordningen börjar gälla ändras även flera EU-direktiv på finansmarknadsområdet[4]. Ändringarna i de olika EU-direktiven syftar främst till att undvika dubbelreglering.

Dora-förordningen ska i vissa avseenden kompletteras av nationell lagstiftning. Regeringen beslutade den 15 augusti 2024 lagrådsremissen Digital operativ motståndskraft för finanssektorn, som bland annat innehåller ett förslag till lag med kompletterande bestämmelser till Dora-förordningen och förslag till ändringar i ett flertal rörelselagar på det finansiella området. Lagändringarna föreslås träda i kraft den 17 januari 2025, samtidigt som Dora-förordningen och de tekniska standarderna ska börja tillämpas i medlemsstaterna. Föreskrifterna och de allmänna råden föreslås träda i kraft vid samma tidpunkt.

EU:s förordning om marknader för finansiella instrument[5] (Mifir) har ändrats genom en förordning[6] 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 i Mifir. FI behöver därför justera i Finansinspektionens föreskrifter (FFFS 2007:17) om verksamhet på marknads-

[2] Europaparlamentets och rådets förordning (EU) 2022/2554av 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
[3] I Dora-förordningen används begreppet ”finansiella entiteter”.
[4] 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.
[5] Europaparlamentets och rådets förordning 600/2014/EU av den 15 maj 2014 om marknader för finansiella instrument.
[6] 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.

platser (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.

Föreskriftsprojektet har följande mål.

Till den del projektet handlar om justeringar i befintliga föreskrifter är målet 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 är korrekta och språkbruket enhetligt. Till en begränsad del har de föreslagna ändringarna i föreskrifterna som mål att företagens verksamhetsplaner ska innehålla ytterligare information. Syftet med de föreslagna 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.

Till den del projektet handlar om att införa nya föreskrifter är målet att möjliggöra för FI att dels på ett effektivt sätt ta emot de uppgifter som ska lämnas in enligt i Dora-regelverket, dels kunna vidarerapportera uppgifterna till de europeiska tillsynsmyndigheterna.

Om föreskriftsprojektets mål uppnås, bidrar det till att FI kan uppfylla sitt övergripande mål för det finansiella systemet.

1.2 Nuvarande och kommande regelverk

De föreslagna nya och ändrade föreskrifterna är en följd av Dora-förordningen, de tekniska standarder som kommer att tas fram i anslutning till den, och den kompletterande nationella lagstiftningen samt ändringar i berörda rörelselagar. De föreslagna ändringarna i marknadsplatsförskrifterna (se nedan) föranleds delvis av ändringar i Mifir.

Några ytterligare författningsändringar som påverkar föreskriftsprojektet 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

I lagrådsremissen Digital operativ motståndskraft för finanssektorn (se s. 77 och 78) bedömer regeringen att den själv, eller den myndighet som den bestämmer, kan 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 och när dessa uppgifter ska lämnas.

Regeringen föreslår inte att det ska lämnas något bemyndigande i lag att meddela sådana föreskrifter, eftersom den anser att sådana föreskrifter är att anse som verkställighetsföreskrifter, som regeringen kan meddela utan något bemyndigande i lag. Regeringen uttalar vidare att det finns skäl att införa reglering såväl om formatet för rapportering som tid som sätt för rapportering uppgifter om tredjepartsleverantörer av IKT-tjänster. I denna remisspromemoria gör FI därför antagandet att regeringen i en förordning kommer att lämna ett bemyndigande för FI att meddela föreskrifter i de nämnda delarna. Om regeringen gör det så kommer FI att ha möjlighet att

meddela sådana föreskrifter om rapportering som föreslås i denna remiss-promemoria.

FI kommer att följa Regeringskansliets arbete och anpassa sin regelgivning i enlighet med de bemyndiganden som finns eller, i förekommande fall, införs.

1.4.2 Ändringar av befintliga föreskrifter och allmänna råd

De föreskrifter och allmänna råd som anges nedan i punkterna a–k är sådana som FI föreslår ska ändras. Av lagrådsremissen Digital operativ motståndskraft för finanssektorn framgår att regeringen inte föreslår några ändringar i de bemyndiganden som ligger till grund för de föreskrifterna och allmänna råden.

De föreslagna 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 verksamhetsplanen eller i rutiner till följd av Dora-förordningen. Nedan anges vilka bemyndiganden som FI kan stödja sig på för att göra dessa föreskriftsändringar.

a) Finansinspektionens föreskrifter (FFFS 2007:17) om verksamhet på marknadsplatser, nedan *marknadsplatsföreskrifterna.* Bemyndigande för att göra de föreslagna ändringarna 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*. Bemyndigande för att göra de föreslagna ändringarna 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*. Bemyndigande för att göra de föreslagna ändringarna finns i 6 § 2, 8, 9 och 11 förordningen (2011:776) om elektroniska pengar.
d) Finansinspektionens föreskrifter (FFFS 2013:9) om värdepappersfonder, nedan *värdepappersfondsföreskrifterna*. Bemyndigande för att göra de föreslagna ändringarna 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*. Bemyndigande för att göra de föreslagna ändringarna finns i 4 § 4

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*. Bemyndigande för att göra de föreslagna ändringarna 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*. Bemyndigande för att göra de föreslagna ändringarna finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse och 6 kap. 1 § 9 och 13 förordningen (2007:572) om värdepappersmarknaden.
h) Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem, nedan *it-föreskrifterna*. Bemyndigande för att göra de föreslagna ändringarna finns i 5 kap. 2 § 5 förordningen (2004:329) om bank- och finansieringsrörelse.
i) Finansinspektionen föreskrifter och allmänna råd (FFFS 2018:4) om verksamhet för betaltjänstleverantörer, nedan *föreskrifterna om betaltjänstverksamhet*. Bemyndigande för att göra de föreslagna ändringarna finns i 5 § 13, 14 och 16 förordningen (2010:1008) om betaltjänster.
j) Finansinspektionens föreskrifter och allmänna råd (FFFS 2019:21) om tjänstepensionsföretag, nedan *tjänstepensionsföreskrifterna*. Bemyndigande för att göra de föreslagna ändringarna finns i 5 kap. 2 § 27 förordningen (2019:809) om tjänstepensionsföretag.
k) Finansinspektionens föreskrifter (FFFS 2024:5) om clearing och avveckling av betalningar, nedan *clearingföreskrifterna*. Bemyndigande för att göra de föreslagna ändringarna finns i 4 § 4 förordningen (2024:127) om clearing och avveckling av betalningar.

1.5 Ärendets beredning

Arbetet med att ta fram de föreslagna föreskrifterna 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.

2 Motivering och överväganden

FI föreslår att det ska införas nya föreskrifter (Dora-föreskrifterna) samt att det ska göras ett antal ändringar i befintliga föreskrifter och allmänna råd. I avsnitten 2.2–2.4 redovisas förslagen till nya och ändrade föreskrifter och allmänna råd samt vilka överväganden som FI gör.

2.1 Nya föreskrifter med anledning av Dora-förordningen

***Finansinspektionens förslag*:** Nya föreskriftsbestämmelser införs om att sådana finansiella entiteter som avses i Dora-förordningen ska rapportera allvarliga IKT-relaterade incidenter och betydande cyberhot till FI på det sätt som anges på FI:s webbplats. Det införs också en föreskriftsbestämmelse om att finansiella entiteterna varje år ska skicka in hela sitt informationsregister till FI på det sätt som anges på FI:s webbplats. Rapporteringen av informationsregister ska ha kommit in till Finansinspektionen senast den 28 februari varje år och gälla förhållandena vid utgången av föregående kalenderår**.**

***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 lämna det fullständiga informationsregistret, eller särskilt angivna delar av det.

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 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 föreslår därför att företagen ska komma in med ovan nämnda rapporteringar 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 bör införas av den

innebörden. Det format som anges på FI:s webbplats kommer att stämma överens med det format som de europeiska tillsynsmyndigheterna har anvisat de behöriga myndigheterna att använda vid vidarerapporteringen.

FI föreslår vidare att det ska införas en föreskriftsbestämmelse om att de finansiella entiteterna ska rapportera informationsregister till FI första gången senast den 28 februari 2025, och därefter samma tidpunkt varje år. De föreslagna tidpunkterna för rapporteringen bedöms ge FI tillräckligt med tid att för att säkerställa korrekt överföring av informationen till de europeiska tillsynsmyndigheterna, utifrån vad som kan antas om när FI kan behöva göra vidarerapporteringen.

De föreslagna rapporteringstidpunkterna kan komma att justeras, eftersom det ännu inte är känt vilka tidpunkter som kommer att gälla för FI:s vidarerapportering av uppgifter till de europeiska tillsynsmyndigheterna.

De nya rapporteringsbestämmelserna bör samlas i en ny författning, Finansinspektionens föreskrifter om rapportering av incidenter och informationsregister enligt EU:s förordning om digital operativ motståndskraft för finanssektorn.

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

***Finansinspektionens förslag*:** Den incidentrapportering som ska ske enligt Dora-förordningen inte ska 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.

***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-förord-

ningen. FI föreslår 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.

2.3 Ändringar i befintliga föreskrifter

2.3.1 Marknadsplatsföreskrifterna

***Finansinspektionens förslag*:** 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.

***Finansinspektionens skäl*:** Marknadsplatsföreskrifterna gäller för bland annat börser och värdepappersinstitut som också omfattas av Dora-förordningens tillämpningsområde (se artikel 2.1 i och e). De föreskrifterna behöver därför anpassas så att den verksamhetsplan som lämnas in i samband med en ansökan innehåller uppgifter om hur företaget ska uppfylla vissa krav i Dora-förordningen.

FI föreslår att en hänvisning till Dora-förordningen införs i 1 a kap. 20 § andra stycket 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 föreslår vidare att en ny bestämmelse införs 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 föreslås 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 föreslås bli justerade så att de inte gäller 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 föreslås för rapportering av händelser av väsentlig betydelse, föreslås även en justering av 1 a kap. 21 § 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, föreslår FI att 1 a kap. 28 § ändras 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 8 a och 8b i Mifir. Därmed kan ansökan om tillstånd återspegla de krav som ställs på verksamheten enligt Mifir.

2.3.2 Betaltjänstföreskrifterna

***Finansinspektionens förslag*:** 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.

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

Enligt 2 kap. 16 och 16 a §§ ska ett företag i den verksamhetsplan som ska ges in samband med en ansökan om tillstånd ange hur dess it-verksamhet 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, föreslår FI att en hänvisning till förordningen införs i 2 kap. 16 och 16 a §§.

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, inklusive krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering bör 10 kap. inte gälla för sådana uppdragsavtal som regleras i Dora-förordningen. FI föreslår därför att 10 kap. 1 § kompletteras med en hänvisning till Dora-förordningen för att tydliggöra att kapitlet inte ska tillämpas på uppdragsavtal som omfattas av kapitel V i Dora-förordningen. 10 kap. ska alltjämt tillämpas på andra uppdragsavtal än de som omfattas av Dora-förordningen.

I 12 kap. 4 § finns 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. Den sistnämnda bestämmelsen föreslås upphöra att gälla (se avsnitt 2.3.9). Därför behöver även 12 kap. 4 § i de nu aktuella föreskrifterna tas bort.

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

2.3.3 E-pengaföreskrifterna

***Finansinspektionens förslag*:** E-pengaföreskrifternas bestämmelser om verksamhetsplanens innehåll i fråga om it-verksamhet och rutiner för rapportering av händelser av väsentlig betydelse ska 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 ska införas en definition av Dora-förordningen i föreskrifterna.

***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 innehåller uppgifter om hur ett företag följer Dora-förordningen, föreslår FI att tillägg av den innebörden införs i den bestämmelse som reglerar vad en sådan verksamhetsplan ska innehålla (2 kap. 15 §). Vidare bör företaget i verksamhetsplanen redogöra för vilka rutiner det har för att rapportera betalningsrelaterade operativa incidenter och säkerhetsincidenter enligt artikel 19 i Dora-förordningen. Ett tillägg av den innebörden bör göras i den bestämmelse i e-pengarföreskrifterna (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 att uppdrag ska regleras i skriftliga avtal samt bestämmelser 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 inklusive krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering bör 8 kap. inte gälla för sådana uppdragsavtal som

regleras i Dora-förordningen. FI föreslår därför att 8 kap. 1 § 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.

I 10 kap. 4 a § finns 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, en bestämmelse som FI nedan (se avsnitt 2.3.9) föreslår ska upphöra att gälla. Därför behöver även 10 kap. 4 a § i de nu aktuella föreskrifterna tas bort.

Eftersom det föreslås att hänvisningar ska göras till Dora-förordningen på ett antal ställen i föreskrifterna, föreslås också en definition av förordningen ska införas i det inledande kapitlet.

2.3.4 Värdepappersfondföreskrifterna

***Finansinspektionens förslag*:** 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 i föreskrifterna om uppdragsavtal ska inte gälla för hantering av IKT-tredjepartsrisker enligt kapitel V i Dora-förordningen.

Det ska införas en definition av Dora-förordningen i föreskrifterna.

***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 bör göras i bestämmelserna om ett fondbolags verksamhetsplan, av den innebörden att det ska framgå av verksamhetsplanen hur ett företag uppfyller kraven i Dora-förordningen om hantering av hantering av IKT-tredjepartsrisker.

FI föreslår att kraven på vad en verksamhetsplan ska innehålla i fråga om uppdragsavtal och it-verksamhet (2 kap. 11 och 12 §§) kompletteras med hänvisningar till Dora-förordningen för att tydliggöra att även uppgifter i förhållande till 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 föreslår 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 föreslår 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 föreslår därför att det i 10 kap. 1 § ska anges att kapitlet inte gäller 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 värdepappersfondsföreskrifterna finns bestämmelser om uppdragsavtal. Bland annat innehåller kapitlet bestämmelser om att uppdrag ska regleras i skriftliga avtal och om utformningen 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 föreslår FI att 14 kap. inte ska gälla för sådana uppdragsavtal som regleras i Dora-förordningen. 14 kap. ska alltjämt tillämpas för andra uppdragsavtal än de som omfattas av Dora-förordningen.

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

2.3.5 AIF-förvaltarföreskrifterna

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

***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 bör därför kompletteras 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 det föreslås att det ska hänvisas till Dora-förordningen på ett antal ställen i föreskrifterna, föreslås även en definition av förordningen i det inledande kapitlet.

2.3.6 SRK-föreskrifterna

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

Bestämmelser 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.

***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.

Bestämmelsen i 2 kap. 2 § i föreskrifterna bör upphöra att gälla, eftersom paragrafen innehåller krav på att företag ska ha ändamålsenliga it-system med mera som innebär en dubbelreglering i förhållande till artikel 7 och 9 i Dora-förordningen. I de artiklarna fina som 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.

FI föreslår även att det i 2 kap. införs en begränsning 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.

3 kap. i föreskrifterna gäller styrelsens och den verkställande direktörens ansvar. Kapitlet handlar bland annat om styrelsens ansvar över strategier och uppdatering av interna regler. Kapitel II i Dora-förordningen innehåller krav som delvis överlappar med de krav som anges i föreskrifterna. För att undvika dubbelreglering föreslår FI att det införs en begränsning i föreskrifternas tillämpningsområde, som innebär att 3 kap. inte ska tillämpas på hantering av IKT-risker som enligt i kapitel II i Dora-förordningen.

FI föreslår att termen ”it-system” ska tas bort i 5 kap. 4 §. 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 hanterar IKT-risker och gör en risk-

bedömning vid varje större förändring av nätverks- och informationssystemets infrastruktur.

5 kap. i 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 föreslår därför att det införs en begränsning i 5 kap. i föreskrifternas tillämpningsområde som innebär att föreskrifterna inte gäller för sådan hantering av IKT-risker som avses i Dora-förordningen

I 10 kap. i 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) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering föreslår FI att 10 kap. inte ska gälla för sådana uppdragsavtal som regleras i Dora-förordningen. 10 kap. ska alltjämt tillämpas för andra uppdragsavtal än de som omfattas av Dora-förordningen.

Eftersom det ska införas hänvisningar till Dora-förordningen på ett antal ställen i föreskrifterna, bör det även införas en definition av förordningen i det inledande kapitlet. Mot bakgrund av de ändringar som föreslås, får vissa bestämmelser en ny beteckning och rubriker placeras framför en annan paragraf än tidigare.

2.3.7 Föreskrifterna om operativa risker

***Finansinspektionens förslag*:** 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.

Upplysningsbestämmelsen om bestämmelserna om informationssäkerhet (5 kap. 8 §), bestämmelsen om it-system (5 kap. 9 §) och bestämmelsen om huvudsakligt it-driftställe (5 kap. 19 §) ska upphöra att gälla.

Därutöver görs redaktionella ändringar.

***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.

Det bör läggas till en begränsning för föreskrifternas tillämpningsområde i 1 kap. 2 §, 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.

Bestämmelserna i 5 kap. 8 och 9 §§ bör upphöra 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. it-föreskrifterna. Dessa hänvisningar behöver tas bort eftersom FI föreslår att 2 och 3 kap. i it-föreskrifterna ska upphöra att gälla (se avsnitt 2.4.8 nedan).

Termen ”it-system” bör tas bort i följande paragrafer: 3 kap. 1 § samt nuvarande 5 kap. 10 och 14 §§. Skälet till att ta bort termen är att tydliggöra att bestämmelser om operativa risker med knytning till it-system ska hanteras enligt Dora-förordningen för de företag som faller inom Dora-förordningens tillämpningsområde.

Bestämmelsen i 5 kap. 19 § bör upphöra 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 strategier och förfaranden för säkerhetskopiering och bör 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 förslag*:** It-föreskrifterna upphävs och ersätts av nya 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.

***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, till exempel Europeiska bankmyndigheten Eba, rörande operativa risker och hanteringen av till exempel säkerhetsrisker och informationssäkerhetsarbete, till svenska författningsbestämmelser.

Dora-förordningen i 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 skulle uppstå om inte bestämmelserna i it-föreskrifterna som tar upp de ämnena upphör att gälla. Av det skälet föreslås att bestämmelserna i 2 kap., 3. kap, och 4 kap. 3 och 5 §§ it-föreskrifterna ska utmönstras.

Eftersom detta innebär att huvuddelen av bestämmelserna i it-föreskrifterna ska tas bort, föreslås att it-föreskrifterna upphävs 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.

[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

2.3.9 Föreskrifterna om betaltjänstverksamhet

Finansinspektionens förslag: 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.

***Finansinspektionens skäl*:** Föreskrifterna om betaltjänstverksamhet gäller för kreditinstitut, betalningsinstitut, registrerade betaltjänstleverantörer, institut för elektroniska pengar, och registrerade utgivare av elektroniska pengar, som 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 bör tas bort, eftersom det kommer att utgöra en dubbelreglering i förhållande till artikel 7 och 9 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 bör det införas 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 föreslår 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.

Redaktionella ändringar bör ske i 6 kap. i föreskrifterna på så sätt att rubriker flyttas och paragrafer ändrar beteckning, så att bestämmelserna placeras i löpande ordningsföljd. Som en följd av att bestämmelser i kapitlet upphävs och flyttas behöver också vissa hänvisningar ändras.

2.3.10 Tjänstepensionsföreskrifterna

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

***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. 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 inklusive krav på kontraktsmässiga arrangemang (uppdragsavtal) i artikel 28.4 och på avtalsbestämmelser i artikel 30. För att undvika dubbelreglering bör det i föreskrifterna införas en bestämmelse om att 8 kap. 69, 70 och 71 §§ inte ska gälla för sådana uppdragsavtal som regleras i Dora-förordningen. Denna bestämmelse bör placeras i 8 kap. 2 §.

Bestämmelserna i föreskrifterna om uppdragsavtal ska alltjämt gälla för andra uppdragsavtal än sådana som avses i Dora-förordningen.

2.3.11 Clearingföreskrifterna

Finansinspektionens förslag: 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.

Finansinspektionens skäl: Clearingbolag omfattas inte av Dora-förordningens tillämpningsområde. Dessa bolag bör alltså även i fortsättningen omfattas av föreskriftskrav när det gäller deras it-system.

När det gäller styrning och riskhantering görs relativt omfattande hänvisningar till SRK-föreskrifterna och föreskrifterna om operativa risker. De föreskrifterna föreslås nu bli ändrade (se avsnitt 2.3.6 och 2.3.7). Dessa föreslagna ändringar skapar 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 föreslås bli ändrade så att bestämmelserna inte längre omfattar it-system, bör nya bestämmelser tas in i clearingföreskrifterna som motsvarar den nuvarande lydelsen av de bestämmelserna. I annat fall skulle föreskriftskraven på clearingbolagen falla bort till den del de avser it-system.

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 § clearingföreskrifterna, varför det saknas skäl att i clearingföreskrifterna införa bestämmelser som motsvarar 5 kap. 10 § andra stycket och 5 kap. 11 § andra stycket föreskrifterna om operativa risker.

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

2.4 Ikraftträdande- och övergångsbestämmelser

Finansinspektionens förslag: De nya och ändrade föreskrifterna och allmänna råden ska träda i kraft ska träda i kraft den 17 januari 2025.

Den första rapporteringen av informationsregister ska ske senast den 28 februari 2025. Rapporteringen ska då avse förhållandena den 31 januari 2025.

Finansinspektionens skäl: De nya och ändrade föreskrifterna och allmänna råden hänger mycket nära samman med Dora-förordningen och den kompletterande reglering som föreslås bli införd på lagnivå. Finansinspektionens nya reglering bör därför träda i kraft vid samma tidpunkt som Dora-förordningen börjar gälla i medlemsstaterna och den kompletterande svenska lagregleringen föreslås träda i kraft, dvs den 17 januari 2025.

Det är angeläget att rapporteringen av informationsregister enligt de nya föreskrifterna om rapportering av incidenter och informationsregister enligt EU:s förordning om digital operativ motståndskraft för finanssektorn kommer i gång så snart som möjligt. Den första rapporteringen av informationsregister bör därför ske senast den 28 februari 2025. Eftersom Dora-förordningen inte kommer att ha börjat gälla vid årsskiftet 2024/2025 bör den första rapporteringen av informationsregister inte avse förhållandena vid det årsskiftet. I stället bör den avse förhållandena vid det första månadsskiftet efter det att Dora-förordningen har börjat gälla, dvs. den 31 januari 2025.

3 Förslagets konsekvenser

3.1 Inledning

De nya och ändrade föreskrifterna och allmänna råden som FI föreslår är en följd av Dora-förordningen. Företagen som anges nedan i punkterna a–s är sådana företag som omfattas av Dora-förordningen och som kommer att beröras 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.

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. När det gäller krav på tekniskt format för företagens inrapportering och vid vilken tidpunkt som företagen ska göra en sådan rapportering, saknas det förutsättningar i Dora-förordningen för att ta särskild hänsyn till förutsättningarna för små företag.

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 de föreslagna 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, konkurrensförmåga eller villkor i övrigt.

De nya och ändrade föreskrifterna föreslås träda i kraft samtidigt som Dora-förordningen. FI bedömer inte att det är möjligt att ta någon särskild hänsyn

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

vid fastställandet av tidpunkten för ikraftträdande. När det gäller tekniskt format för inrapportering och tidpunkt för inrapportering av informationsregister, bedömer FI att det finns behov av särskilda informationsinsatser till berörda företag.

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

3.2 Konsekvenser för samhället och konsumenterna

Varken de föreslagna nya eller ändrade föreskrifterna bedöms påverka konkurrensen mellan företagen på marknaden eller medföra några konsekvenser för konsumenterna.

3.3 Konsekvenser för företagen

FI redogör nedan för de konsekvenser som de föreslagna 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. 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 ett 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 tio – tjugo 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 rapporteringstillfällen, då referenstidpunkt är 31 januari 2025). Detta medför en årlig kostnad för att granska och skicka in uppgifterna till FI, som i sin tur ska vidarebefordra informationen till EU-tillsynsmyndigheterna. FI uppskattar att företagens kostnader för att varje år skicka in uppgifterna till 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.

[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.

3.3.3 Konsekvenser av föreslagna ändringar i befintliga föreskrifter

De föreslagna 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 de föreslagna ändringarna innebär att företagens verksamhetsplan ska innehålla viss angiven information, behöver företagen se över om det behövs göra nödvändiga uppdateringar. FI uppskattar att denna kostnad uppgår till mellan 7 500 och 15 000 kronor (cirka 5 till 10 timmar à 1531 kr), i form av en engångskostnad.

När det gäller förslaget till ändring av 1 a kap. 28 § marknadsplatsföreskrifterna gäller 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

De föreslagna 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.